Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Μεταπτυχιακή Διατριβή
Στην Ασφάλεια Υπολογιστών και Δικτύων

Ασφάλεια και ιδιωτικότητα σε έξυπνες εφαρμογές εγγύτητας κρουσμάτων του COVID-19

ΣΩΤΗΡΙΑ ΤΡΙΑΝΤΑΦΥΛΛΙΑ ΣΩΤΗΡΧΟΥ

Επιβλέπων Καθηγητής

ΚΩΝΣΤΑΝΤΙΝΟΣ ΛΙΜΝΙΩΤΗΣ

Μάιος 2021

Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Ασφάλεια και ιδιωτικότητα σε έξυπνες εφαρμογές εγγύτητας κρουσμάτων του COVID-19

ΣΩΤΗΡΙΑ ΤΡΙΑΝΤΑΦΥΛΛΙΑ ΣΩΤΗΡΧΟΥ

Επιβλέπων Καθηγητής
ΚΩΝΣΤΑΝΤΙΝΟΣ ΛΙΜΝΙΩΤΗΣ

Η παρούσα μεταπτυχιακή διατριβή υποβλήθηκε
προς μερική εκπλήρωση των απαιτήσεων για απόκτηση

μεταπτυχιακού τίτλου σπουδών
στην Ασφάλεια Υπολογιστών και Δικτύων

από τη Σχολή Θετικών και Εφαρμοσμένων Επιστημών
του Ανοικτού Πανεπιστημίου Κύπρου

Μάιος 2021

Περίληψη

"If you have nothing to hide, you have nothing to fear"

Η τελευταία εξάπλωση του Κορωναιού SARS-CoV-2/Covid-19 , ο οποίος πήρε το όνομά του από το έτος που εμφανίστηκε, έχει προκαλέσει παγκόσμια αναταραχή τόσο στο υγειονομικό όσο και στο οικονομικό σκηνικό. Επιχειρήσεις έκλειναν, εργαζόμενοι απολύονταν από φόβο μήπως έχουν προσβληθεί από τον ιό. Οι κυβερνήσεις σε όλο τον κόσμο προέβηκαν σε lockdown για να αντιμετωπίσουν την κατάσταση που από την αρχή της ακόμα φάνταζε και ήταν τρομαχτική. Λόγω της εξαιρετικά μεταδοτικής φύσης του ιού, η κοινωνική αποστασιοποίηση είναι ένα θεμελιώδες μέτρο που έχει ήδη υιοθετηθεί από πολλές χώρες.

Το πιο δύσκολο για αυτόν τον ιό είναι η ιχνηλάτηση των επαφών ενός μολυσμένου ατόμου και για αυτόν τον λόγο οι κυβερνήσεις έχουν δείξει μεγάλο ενδιαφέρον στη δημιουργία εφαρμογών οι οποίες θα ιχνηλατούν τις επαφές του χρήστη για τις οποίες είναι ενήμερος και για κάποιες που μπορεί να μην είναι. Οι εφαρμογές αυτές στόχο έχουν την αντιμετώπιση της πανδημίας και τη μείωση της εξάπλωσής της με γνώμονα πάντα την προστασία των προσωπικών τους δεδομένων. Χωρίς προσεκτικές εκτιμήσεις, η ιχνηλάτηση επαφών μπορεί να μετατραπεί σε ένα τεράστιο εργαλείο παρακολούθησης, καταπατώντας την ιδιωτικότητα του ατόμου. Αυτό που κάνει τα πράγματα πιο δύσκολα είναι ότι ο τρόπος που χρησιμοποιούν τις εφαρμογές ιχνηλάτησης η εκάστοτε χώρα και οι κυβερνήσεις και εξαρτάται σε μεγάλο βαθμό από την αντίληψη της ιδιωτικής ζωής, από το πολιτικό καθεστώς και την υποκείμενη κουλτούρα τους.

Στη συγκεκριμένη διατριβή θα αναφέρουμε εφαρμογές που ήδη υπάρχουν ανά τον κόσμο, σε ποιες κατηγορίες διακρίνονται βάση πρωτοκόλλων που χρησιμοποιούν και ποια θέματα εμπιστευτικότητας εγείρονται. Περαιτέρω, οι πιο γνωστές εφαρμογές μελετώνται, με χρήση κατάλληλων εργαλείων λογισμικών, ως προς τη λειτουργία τους σε πραγματικό χρόνο, με σκοπό να διαπιστωθεί τόσο η ευχρηστία (φιλικότητα προς το χρήστη) και η αποτελεσματικότητά τους, όσο και τυχόν ζητήματα ιδιωτικότητας που εγείρουν.

Summary

The latest spread of the Corona SARS-CoV-2 / Covid-19, which took its name from the year it appeared, has caused global turmoil in both the health and economic scene. Businesses were closing, workers were being fired for fear of being infected with the virus. Governments around the world have locked in to deal with what has been a frightening situation since its inception. Doctors and authorities have not figured out how the virus is transmitted or why some people get sick and some do not. All they know is that it is a terribly infectious virus and the only "weapon" that people have is to wear masks and keep their distance. Research has shown that if people are less than a meter apart and without a mask they are more likely to get sick, if they one is wearing they are less likely to be sick and if they are both wearing they are even less likely to get sick.

The most difficult thing for this virus is to track the contacts of an infected person and for this reason governments have shown great interest in creating applications that will track the contacts of the user of which he is aware and for some who may not be. These applications aim to address the pandemic and reduce its spread, always with the protection of their personal data in mind. Without careful consideration, tracking contacts can become a huge tracking tool, violating an individual's privacy. What makes things more difficult is that the way in which, countries and governments use tracking applications depends to a large extent on their perception of privacy, their political status and their underlying culture.

In this dissertation we will study applications that already exist around the world, in which categories they are distinguished based on protocols they use and which confidentiality issues are raised. Moreover, the most known such applications are analyzed in real- time operation, through appropriate software tools, in order to determine both their usability (user friendliness) and their effectiveness as well as possible privacy issues that arise.

Ευχαριστίες

Καταρχάς θα ήθελα να ευχαριστήσω τον καθηγητή μου κ. Κωνσταντίνο Λιμνιώτη για τη βοήθεια και τις συμβουλές που μου παρείχε καθ' όλη τη διάρκεια της παρούσης διατριβής. Πρόκειται για έναν εξαίρετο άνθρωπο και έναν εξαίρετο επιστήμονα. Η εμπιστοσύνη που μου έδειξε εξ' αρχής, αναθέτοντάς μου το συγκεκριμένο θέμα αποτέλεσε για εμένα δέσμευση και καθήκον για την επιτυχή περάτωσή του. Το αμείωτο ενδιαφέρον του, η συνεχής υποστήριξή του και η ευγένειά του, αποτέλεσαν πηγή έμπνευσης και δύναμης καθ' όλη την προσπάθεια ολοκλήρωσης της παρούσης διατριβής.

Στη συνέχεια θα ήθελα να ευχαριστήσω τους γονείς μου και τα παιδιά μου για την υπομονή που έδειξαν όλο αυτό το διάστημα που διήρκησε η διατριβή. Χωρίς τη συμπαράσταση και την υποστήριξή τους δεν θα είχα ολοκληρώσει τον στόχο μου.

Θα ήθελα επίσης να ευχαριστήσω τους φίλους μου Χρήστο και Αριστέα για όλο το υλικό που μου παρείχαν, για όλες τις συμβουλές και την κατανόησή τους.

Τέλος θα ήθελα να ευχαριστήσω ολόθερμα τη Ναταλία Βαξεβάνου, για την πολύτιμη βοήθειά της, τις συμβουλές της, για την ευγένεια αλλά και την ανιδιοτελή καλοσύνη της.

ΠΕΡΙΕΧΟΜΕΝΑ

i

Κεφάλαιο 1

Εισαγωγή

Η χρονιά που πέρασε 2019-2020 θα μείνει στην ιστορία από το μεγάλο ξέσπασμα της πανδημίας της αναπνευστικής νόσου 2019-nCov, η οποία είναι μια μολυσματική ασθένεια που προκαλείται από τον κορωναϊό SARS-CoV-2. Ο ιός εντοπίστηκε για πρώτη φορά στην πόλη Γιουχάν της Κίνας στα τέλη του 2019 και έγινε γνωστός στον Παγκόσμιο Οργανισμό Υγείας στις 31 Δεκεμβρίου του 2019 ο οποίος με τη σειρά του στις 30 Ιανουαρίου του 2020 τον δήλωσε ως έκτακτη ανάγκη διεθνούς ανησυχίας για τη δημόσια υγεία. Από τότε έχει διασπαρθεί σε όλον τον πλανήτη και έχει εξελιχθεί σε πανδημία. Η εξάπλωση της πανδημίας έχει αλλάξει τον τρόπο ζωής των ανθρώπων σε όλον τον κόσμο αναγκάζοντας τις κυβερνήσεις να οδηγούν τις χώρες τους σε απαγόρευση κυκλοφορίας, σε αυτοαπομόνωση των ανθρώπων, σε τηλεργασία, να επιβάλλουν τη χρήση μάσκας όταν κυκλοφορούν έξω και να επιβάλλουν στις εταιρείες να διενεργούν συνεχώς διαγνωστικά τεστ στους εργαζομένους τους με στόχο τη μείωση της εξάπλωσής της.

Επειδή οι υγειονομικές αρχές δεν έχουν καταλήξει στο γιατί κάποιοι άνθρωποι νοσούν και κάποιοι όχι, προτείνουνε σε όλους να κρατάνε αποστάσεις και να φοράνε μάσκες για να μη νοσήσουν. Εάν κάποιος νοσήσει δηλώνει στις υγειονομικές αρχές τις επαφές των τελευταίων 14ων ημερών για να γίνει ιχνηλάτηση του ιού και να μειωθεί η εξάπλωσή του. Τα άτομα που θεωρούνται επαφές μένουν σε καραντίνα και μόνο εάν έχουν σοβαρά συμπτώματα νοσηλεύονται. Είναι όμως αρκετά δύσκολο για τον κόσμο να γνωρίζει ακριβώς με ποια άτομα έχει έρθει σε επαφή και για πόση ώρα και ποια από αυτά τα άτομα θεωρούνται όντως επαφή (αυτό εξαρτάται από το αν έχουν βρεθεί σε εξωτερικό ή εσωτερικό χώρο, αν φορούσαν μάσκα και για πόση ώρα βρέθηκαν κοντά και φυσικά τι εννοούμε όταν λέμε ότι ήταν «κοντά»). Βέβαια υπάρχουν και αυτοί που είτε από φόβο είτε από ντροπή δεν αποκαλύπτουν στις υγειονομικές αρχές τα άτομα που έχουν έρθει σε επαφή με αποτέλεσμα να μη γίνεται και πάλι σωστή ιχνηλάτηση.

Όλη αυτή η κατάσταση, έθεσε την ανάγκη στο κράτος και στην κοινωνία να ιχνηλατεί τις επαφές των ασθενών χρησιμοποιώντας «έξυπνες» εφαρμογές ώστε να παρακολουθούν την εξάπλωσή του διασφαλίζοντας την οικονομία και την ανθρώπινη εργασία. Ο στόχος των «έξυπνων» εφαρμογών είναι να ενημερώσει τον κόσμο για το εάν έχουν έρθει ποτέ σε επαφή με θετικά διαγνωσμένα άτομα ώστε να απομονωθούν αλλά και να κάνουν, αν χρειάζεται, ένα διαγνωστικό τεστ. Μια τέτοια όμως κίνηση πρέπει να συνοδεύεται από μεγάλη προσοχή διότι τα στοιχεία πρέπει να χρησιμοποιούνται μόνο για το σκοπό για τον οποίο εξυπηρετούν και όχι να γίνεται κατάχρηση από τους ίδιους τους χρήστες ή και από το κράτος ,προστατεύοντας έτσι την ιδιωτικότητα των ατόμων και τα θεμελιώδη δικαιώματά τους.

Μέχρι σήμερα υπάρχουν πολλές διαφορετικές τεχνολογίες και προσεγγίσεις ως προς τον τρόπο υλοποίησης και λειτουργίας τέτοιων «έξυπνων» εφαρμογών. Κάποιες είναι κεντρικοποιημένες (δηλαδή οι ασθενείς, οικειοθελώς), «ανεβάζουν» σχετική ψευδωνυμοποιημένη πληροφορία σε μία κεντρική βάση, στην οποία όλοι οι χρήστες έχουν πρόσβαση και μπορούν να δουν πληροφορίες για ύπαρξη κρουσμάτων σε διάφορα μέρη, ενώ άλλες προσεγγίσεις είναι μη κεντρικοποιημένες και βασίζονται σε ανταλλαγές πληροφοριών μεταξύ «έξυπνων» συσκευών. Περαιτέρω, η ιχνηλάτηση μπορεί να γίνεται είτε βάσει πληροφοριών γεωγραφικής τοποθεσίας (GPS) είτε βάσει ανταλλαγής δεδομένων με το πρωτόκολλο Bluetooth: πιο προχωρημένες λύσεις προτείνουν την εφαρμογή των λεγόμενων «ασφαλών υπολογισμών» (secure multiparty computations). Δεν είναι ακόμα κοινά αποδεκτό το ποια τεχνική είναι καλύτερη, τόσο ως προς

την σωστή ιχνηλάτηση κρουσμάτων όσο και ως προς την προσβολή της ιδιωτικότητας και της έκθεσης προσωπικών δεδομένων σε κίνδυνο. Επίσης, λόγω του καινοφανούς χαρακτήρα των εφαρμογών, δεν έχουν ακόμα μελετηθεί ενδελεχώς οι εν λόγω εφαρμογές ως προς τι πραγματικά «δικαιώματα» αποκτούν από τη στιγμή που εγκαθίστανται στη συσκευή ενός χρήστη και σε τι είδους πληροφορία σε αυτή, αποκτούν πρόσβαση. Άλλωστε μια εφαρμογή σε μία κινητή συσκευή η οποία έχει γίνει προέκταση του εαυτού μας είναι ίσως η καταλληλότερη λύση για να προστατεύσουμε τον εαυτό μας και τους γύρω μας, χωρίς πολύ κόπο και ως επί το πλείστον ανώνυμα.

1.2 Βασικά Ερευνητικά Ερωτήματα

Η παρούσα διατριβή στόχο έχει να μελετήσει τις εφαρμογές ιχνηλάτησης επαφών COVID-19(contact tracing apps) που υπάρχουν ανά τον κόσμο και πώς οι χρήστες θα μπορούν να τις χρησιμοποιούν με γνώμονα πάντα την προστασία της ιδιωτικότητας τους και των προσωπικών τους δεδομένων.

Οπότε από τη μελέτη αυτή προκύπτουν και τα εξής ερευνητικά ερωτήματα τα οποία και επιχειρήσαμε να τα απαντήσουμε:

- Ποιες τεχνολογίες έχουν μέχρι τώρα χρησιμοποιηθεί για τις εφαρμογές ιχνηλάτησης κρουσμάτων COVID-19 (πώς οι χρήστες θα χρησιμοποιούν τις «έξυπνες» εφαρμογές;)
- Με ποιον τρόπο θα γίνεται η ιχνηλάτηση;
- Ποια τα πλεονεκτήματα και μειονεκτήματα της κάθε μιας;
- Τι ζητήματα ιδιωτικότητας εγείρονται και πώς αυτά αντιμετωπίζονται;
- Ποια ακριβώς επεξεργασία προσωπικών δεδομένων συντελείται κατά τη χρήση αυτών των εφαρμογών; Πληρούνται οι προϋποθέσεις νομιμότητας αναφορικά με το ευρωπαϊκό νομικό πλαίσιο προστασίας δεδομένων;

1.3 Μεθοδολογία

Το αρχικό τμήμα της διατριβής βασίστηκε σε θεωρητική έρευνα λόγω του μεγάλου αριθμού συναφών εφαρμογών, οι οποίες αναπτύχθηκαν ανά τον κόσμο σε λιγότερο από ένα έτος. Έγινε συλλογή, επιλογή και αποτύπωση της κατάλληλης βιβλιογραφίας για την αποτύπωση πληροφοριών που αφορούν τις εφαρμογές ιχνηλάτησης του ιού Covid-19. Βάσει της

υπάρχουσας βιβλιογραφίας και αρθρογραφίας, αναφέρθηκαν ενδελεχώς όλες οι γνωστές υλοποιήσεις στις οποίες βασίζονται οι εφαρμογές ιχνηλάτησης, οι ευπάθειες και τα ελαττώματά τους καθώς επίσης και ποια θέματα ιδιωτικότητας εγείρονται από τη χρήση αυτών των εφαρμογών.

Στη συνέχεια, η θεωρητική έρευνα συνεχίστηκε μελετώντας τους βασικούς κανόνες του Γενικού Κανονισμού Προστασίας Δεδομένων, ο οποίος αποτελεί το κύριο νομικό πλαίσιο για την προστασία προσωπικών δεδομένων στην Ευρωπαϊκή Ένωση. Η μελέτη του Κανονισμού, αλλά και της e-Privacy Οδηγίας, είναι απαραίτητη προκειμένου να υπάρξει μια βάση αναφοράς ως προς τις προϋποθέσεις νόμιμης επεξεργασίας δεδομένων στο πλαίσιο των εφαρμογών ιχνηλάτησης.

Περαιτέρω, προκειμένου να διερευνηθούν σε πραγματικό χρόνο τι ακριβώς υποκείμενη επεξεργασία προσωπικών δεδομένων πραγματοποιείται από τις εν λόγω εφαρμογές και κατά πόσον αυτή είναι διαφανής προς το χρήστη της, πραγματοποιήθηκε πειραματική έρευνα με τρία εργαλεία όπως το exodus, lumen και το pi_maninthemiddle, προκειμένου να διαπιστωθεί, σε ένα ρεαλιστικό περιβάλλον αφενός η ευχέρεια χρήσης των εφαρμογών ιχνηλάτησης, η φιλικότητα προς τον χρήστη και τα προβλήματα που αντιμετωπίστηκαν και αφετέρου να ελεγχθεί η αποτελεσματικότητά τους σε σχέση με την προστασία προσωπικών δεδομένων του.

Η πειραματική έρευνα έγινε με χρήση οικιακού υπολογιστικού συστήματος στο οποίο εγκαταστάθηκαν τα ανωτέρω εργαλεία και με τη χρήση δύο κινητών συσκευών ώστε να υπάρχει μα πιο ρεαλιστική αποτύπωση του συστήματος.

Εν κατακλείδι, το εν λόγω θέμα έχει πολύ έντονο ερευνητικό ενδιαφέρον, ιδίως για τις ημέρες που διανύουμε. Η βιβλιογραφία αν και έχει περάσει μόλις ένας χρόνος από την έξαρση της πανδημίας είναι ανέλπιστα αρκετή για να *θίξουμε* το θέμα αλλά ελλιπής όσον αφορά τα ζητήματα ιδιωτικότητας και προστασίας προσωπικών δεδομένων των χρηστών.

1.4 Δομή της Διατριβής

Στο 2ο κεφάλαιο της διατριβής κάνουμε μια εισαγωγή ως προς τις βασικές έννοιες και λειτουργίες των λεγόμενων «έξυπνων» εφαρμογών κινητών συσκευών, διερευνώντας επίσης και τι ζητήματα ιδιωτικότητας εγείρονται με τη χρήση των εφαρμογών αυτών.

Στο 3ο κεφάλαιο θα αναλύσουμε τις πιο γνωστές εφαρμογές ιχνηλάτησης Covid-19 που ήδη υπάρχουν και χρησιμοποιούνται ανά τον κόσμο. Στο πλαίσιο αυτό, θα μελετήσουμε τεχνολογίες όπως το Bluetooth Low Energy (στο οποίο μετέπειτα θα δούμε ότι στηρίζονται οι περισσότερες από τις εφαρμογές ιχνηλάτησης) και τα λεγόμενα «beacons» τα οποία μεταδίδονται από τη μία συσκευή στη μία άλλη μέσω του Bluetooth. Στο ίδιο κεφάλαιο θα αναλύσουμε τις κατηγορίες στις οποίες χωρίζονται οι εφαρμογές ιχνηλάτησης ανάλογα σε ποια τεχνολογία βασίζονται(κεντρικοποιημένες και αποκεντρωμένες, Bluetooth ή GPS) και στο τέλος του 3ου κεφαλαίου θα αναφέρουμε τα πιο γνωστά συστήματα στα οποία στηρίζονται οι εφαρμογές ιχνηλάτησης βάσει του διαχωρισμού που προαναφέραμε και που χρησιμοποιούνται ευρέως.

Στο 4ο κεφάλαιο θα αναλύσουμε τις ευπάθειες των συστημάτων που μελετήσαμε στο 3ο κεφάλαιο, τις πιο γνωστές επιθέσεις από τις οποίες κινδυνεύουν και θα αναφέρουμε κάποιες λύσεις που προτείνονται από άλλους ερευνητές.

Στο 5ο κεφάλαιο θα κάνουμε μια εισαγωγή το τι είναι η ιδιωτικότητα και το τι ορίζει ο Γενικός Κανονισμός Προστασίας Δεδομένων, θα αναλύσουμε τα νομικά ζητήματα που εγείρονται από τη χρήση των εφαρμογών ιχνηλάτησης.

Στο 6ο κεφάλαιο θα μελετήσουμε, μέσω κατάλληλου πειραματικού περιβάλλοντος και με τη χρήση διαφόρων εργαλείων λογισμικού, κάποιες από τις πιο γνωστές εφαρμογές που χρησιμοποιούνται τόσο στην Ευρώπη όσο και στον υπόλοιπο κόσμο καθώς και αν τελικά λειτουργούν όπως υποστηρίζουν αναφορικά με την προστασία των προσωπικών δεδομένων των χρηστών. Ο στόχος μας είναι να διερευνηθούν οι υποκείμενες επεξεργασίες προσωπικών δεδομένων που πραγματοποιούνται, κατά πόσον είναι διαφανείς προς τους χρήστες καθώς και εάν είναι συμβατές με το ευρωπαϊκό νομικό πλαίσιο προστασίας προσωπικών δεδομένων, με βάση σχετικές κατευθυντήριες γραμμές που έχουν εκδοθεί από το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων.

Τέλος στο 7ο κεφάλαιο θα παρουσιάσουμε τα συμπεράσματά μας σχετικά με την επιτυχία ή όχι των εφαρμογών ιχνηλάτησης καθώς και μελλοντική τους χρήση σε ενδεχόμενες πανδημίες ή σε άλλους τομείς της υγείας.

Κεφάλαιο 2

Έξυπνες Εφαρμογές

2.1 Τι είναι η «έξυπνη» εφαρμογή (smart app)

Η ετικέτα «έξυπνο» έχει εφαρμοστεί σε διάφορες τεχνολογίες τα τελευταία χρόνια από τα «έξυπνα» κινητά, «έξυπνες» συσκευές, «έξυπνα» σπίτια, «έξυπνες» πόλεις, «έξυπνα» αυτοκίνητα και «έξυπνες» εφαρμογές. Αυτή η «έξυπνη» τεχνολογία για την οποία γίνεται λόγος πρόκειται για μια τεχνολογική πρόοδο υλικού και λογισμικού , η οποία αποτελείται από συσκευές που είναι συνδεδεμένες μεταξύ τους μέσω Bluetooth ή μέσω του Διαδικτύου και πλήρως ανιχνεύσιμες με δυνατότητα παρακολούθησής τους μέσω ενός κεντρικού διακομιστή (υπολογιστή κοκ).

2.1.1 «Έξυπνη» εφαρμογή κινητών (mobile smart app)

Με την πρόοδο της τεχνολογίας, ήρθε και η πρόοδος στα κινητά τηλέφωνα τα οποία περάσανε από πολλά στάδια για να φτάσουν σε αυτό που γνωρίζουμε σήμερα. Οι άνθρωποι ολοένα και αγοράζουν κινητά τηλέφωνα και κινητές συσκευές (tablet), με αποτέλεσμα η ζωή και η καθημερινότητά τους να είναι συνυφασμένη μαζί τους , να τις μεταφέρουν όπου κ αν πηγαίνουν και να τις έχουν μόνιμα ενεργοποιημένες και συνδεδεμένες στο διαδίκτυο. Άλλωστε αυτός είναι ο λόγος που παρά την παγκόσμια οικονομική κρίση οι βιομηχανίες έξυπνων συσκευών συνεχίζουν και έχουν μεγάλα έσοδα και αποτελούν από τις μεγαλύτερες βιομηχανίες στον κόσμο. Η εφαρμογή είναι ένα πρόγραμμα λογισμικού που συνήθως «κατεβάζεται» από πλατφόρμες διανομής εφαρμογών όπως το App Store(IOS) και το Google Play Store. Ορισμένες διατίθενται δωρεάν, ενώ άλλες διατίθενται επί πληρωμή, όπου το κέρδος μοιράζεται μεταξύ δημιουργού και πλατφόρμας διανομής. Μπήκε στη ζωή μας τα τελευταία χρόνια με σκοπό να εξυπηρετήσει την εκάστοτε ανάγκη του χρήστη και να απλοποιήσει τον τρόπο ζωής του. Καθώς οι χρήστες στηρίζονται στις κινητές συσκευές τους για την καθημερινή τους ζωή, έχουν χρησιμοποιήσει εκατομμύρια εφαρμογές, κυρίως εφαρμογές παιχνιδιών, διασκέδασης, νέων, εφαρμογών υγείας, επικοινωνίας, και γενικά εφαρμογές κάθε είδους ώστε οι χρήστες να «κάνουν τα πράγματα» με εύκολο, «έξυπνο» και γρήγορο τρόπο. Μέχρι τον Οκτώβριο του 2020, υπήρχαν 3.6 εκατομμύρια εφαρμογές στο Google Play Store. Τα κύρια πλεονεκτήματα της «έξυπνης» εφαρμογής είναι η συμβατότητά της με όλες τις «έξυπνες» συσκευές (smartphone/tablet/android pc), η δυνατότητα χρήσης της ανεξαρτήτως τοποθεσίας καθώς και η φιλικότητα προς το χρήστη και τα κύρια μειονεκτήματά της είναι η άδεια πρόσβασης σε προσωπικά δεδομένα του χρήστη, όπως τις επαφές του τηλεφώνου του, τα αρχεία καταγραφής κλήσεων, τα δεδομένα του Διαδικτύου, το ημερολόγιο του, δεδομένα σχετικά με την τοποθεσία της συσκευής, την χωρητικότητα της μπαταρίας του κοκ και μάλιστα χωρίς απαραίτητα τη συγκατάθεσή του. Άλλες εφαρμογές ζητάνε από τον χρήστη την άδεια να χρησιμοποιήσουν το μικρόφωνό του, το GPS, την κάμερα ή το WiFi με αποτέλεσμα να καθιστά την κινητή συσκευή βορά στα χέρια ενός κακόβουλου χρήστη (εισβολέα) και του είναι και εύκολο να την παρακολουθήσει. Έρευνες δείχνουν ότι οι πληροφορίες αυτές μπορούν να δημιουργήσουν ένα ηλεκτρονικό προφίλ για τον χρήστη με ακεραιότητα περίπου 95% ακριβές.

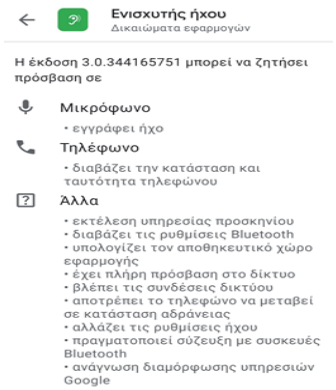
2.2 «Έξυπνες» εφαρμογές και ζητήματα ιδιωτικότητας

Οι «έξυπνες» εφαρμογές, εκ των πραγμάτων, επεξεργάζονται προσωπικά δεδομένα των χρηστών τους. Όπως θα αναφερθεί και στη συνέχεια, προσωπικά δεδομένα δεν θεωρούνται μόνο τα δεδομένα που αφορούν το χρήστη αλλά και δεδομένα που αφορούν την κινητή συσκευή του, την τοποθεσία της, ο αριθμός IMEI της, τα περιβαλλοντικά δεδομένα και δεδομένα που αφορούν τον τρόπο χρήσης της. Στο νομικό πλαίσιο (θα αναλυθεί περαιτέρω στη συνέχεια) έχει πλέον προστεθεί και ο όρος «ψευδωνυμοποίηση» ο οποίος αφορά τη διαδικασία διαχείρισης των δεδομένων χρησιμοποιώντας ψευδώνυμα ή άλλα τεχνητά χαρακτηριστικά ούτως ώστε να μην αποκαλύπτονται τα δεδομένα και συνεπώς η ταυτότητα του ιδιοκτήτη τους. Ωστόσο, από νομική πλευρά, και τα ψευδωνυμοποιημένα δεδομένα αποτελούν προσωπικά δεδομένα και απαιτείται η εκπλήρωση συγκεκριμένων προϋποθέσεων για τη νόμιμη επεξεργασία τους.

Οι εφαρμογές μόλις εγκατασταθούν σε μία κινητή συσκευή, ζητάνε την αποδοχή αδειών ώστε να συνεχίσει η εφαρμογή να λειτουργεί. Άλλες ζητάνε άδεια να χρησιμοποιήσουν το μικρόφωνο και τις επαφές, άλλες ζητάνε την άδεια να έχουν πρόσβαση στις φωτογραφίες της συσκευής , ενώ άλλες ζητάνε άδεια να χρησιμοποιήσουν την τοποθεσία της με την ενεργοποίηση του GPS. Για να είναι μια εφαρμογή συμβατή με τους όρους και τους κανονισμούς του Γενικού Κανονισμού Προστασίας Δεδομένων (ΓΚΠΔ-θα το αναλύσουμε στη συνέχεια) θα πρέπει να ακολουθεί κάποιους κανόνες.

Προφανώς δεν είναι όλες οι εφαρμογές που ζητάνε υποχρεωτικά την αποδοχή του χρήστη για προσβάσεις, «επικίνδυνες» και μη συμμορφούμενες με τις προϋποθέσεις νόμιμης επεξεργασίας. Για παράδειγμα μία εφαρμογή που εγκαθίσταται για να αυξήσει το ηχείο της συσκευής θα πρέπει να έχει πρόσβαση στο ηχείο της. Όπως επίσης μια εφαρμογή των κοινωνικών δικτύων που ζητά την άδεια να χρησιμοποιήσει την τοποθεσία του χρήστη, γιατί θέλει να τη χρησιμοποιεί όταν εκείνος ανεβάζει μια φωτογραφία και για την οποία επιθυμεί να εμφανίζει και πληροφορίες τοποθεσίας, δεν θεωρείται «επικίνδυνη» πρόσβαση.

Υπάρχουν όμως περιπτώσεις που οι εφαρμογές ζητάνε δυσανάλογο αριθμό αδειών (βλ. εικόνα 1) σε σχέση με τις υπηρεσίες που παρέχουν και για το λόγο που αρχικά ο χρήστης επέλεξε να τις εγκαταστήσει, χωρίς να παρέχουν επαρκή πληροφόρηση στο χρήστη για τους σκοπούς των αδειών αυτών. Γιατί για παράδειγμα μια εφαρμογή ήχου να ζητήσει την άδεια όχι μόνο να χρησιμοποιήσει το ηχείο της συσκευής αλλά να εγγράφει ήχο και να «διαβάζει» την κατάσταση του τηλεφώνου του χρήστη;



ΕΙΚΟΝΑ 1: ΆΔΕΙΕΣ ΕΦΑΡΜΟΓΗΣ ΗΧΟΥ

Σε τέτοιες περιπτώσεις, η εφαρμογή δεν δουλεύει σωστά εάν ο χρήστης δεν αποδεχτεί κάθε άδεια πρόσβασης που ζητείται, οπότε ο ίδιος ο χρήστης κατά μία έννοια «εξαναγκάζεται» να αποδεχτεί να χορηγήσει κάθε άδεια πρόσβασης. Πέραν αυτού όμως, το οποίο εγείρει ζητήματα προστασίας προσωπικών δεδομένων, υπάρχουν και περιπτώσεις στις οποίες γίνεται επεξεργασία των δεδομένων η οποία είναι μη διαφανή στο χρήστη και αφορά την αποδοχή για οποιαδήποτε χρήση των δεδομένων από μία τρίτη οντότητα (πέραν του παρόχου της εφαρμογής), όπως εξηγείται και στη συνέχεια.

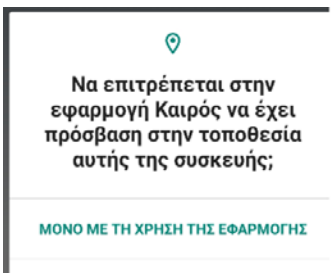
2.3 Δεδομένα που επεξεργάζονται τρίτες οντότητες

Οι «έξυπνες» εφαρμογές χρησιμοποιούν κάποιες βιβλιοθήκες τρίτων (στη διεθνή βιβλιογραφία χρησιμοποιείται ο όρος third-party) για να λειτουργήσουν, οι οποίες με τη σειρά τους μπορούν να ορίσουν τα δικά τους δικαιώματα. Μάλιστα, εάν δύο ή περισσότερες εφαρμογές χρησιμοποιούν τις ίδιες βιβλιοθήκες μπορούν να «ανταλλάσουν» τα δικαιώματά τους με αποτέλεσμα οι εφαρμογές να ζητάνε άδειες που δεν είναι απαραίτητες για τη βασική τους λειτουργία. Σύμφωνα με το[16], οι βιβλιοθήκες τρίτων συνεισφέρουν το 60% ή και παραπάνω του κώδικα των εφαρμογών android και κάθε εφαρμογή χρησιμοποιεί ένα 3.4%-5% των βιβλιοθηκών. Μάλιστα το 73% των εφαρμογών Android μοιράστηκε προσωπικά στοιχεία, όπως διεύθυνση ηλεκτρονικού ταχυδρομείου με τρίτα μέρη, και το 47% των εφαρμογών iOS μοιράστηκε γεωγραφικές συντεταγμένες και άλλα δεδομένα τοποθεσίας με τρίτα μέρη. Οι βιβλιοθήκες αυτές είτε υπάρχουν στο διαδίκτυο σαν ανοιχτός κώδικας όπως το GitHub, BitBucket ή online όπως το Maven είτε δημιουργούνται από άλλες εταιρείες δίνοντας έτσι τη δυνατότητα στους προγραμματιστές να υλοποιήσουν ένα πρόγραμμα γλιτώνοντας χρόνο, πόρους και χρήμα. Τι γίνεται όμως όταν αυτή η τρίτη οντότητα-βιβλιοθήκη έχει ευπάθεια ή κάποια διαρροή

δεδομένων; Η στατική ανάλυση στο[16] έδειξε ότι βιβλιοθήκες τρίτων όπως οι βιβλιοθήκες διαφημίσεων μπορούν να ανακτούν και να εκτελούν κώδικα απευθείας από το διαδίκτυο. Οι κυβερνήσεις αρχίζουν να αντιμετωπίζουν με σοβαρότητα τη συλλογή δεδομένων και την κοινή χρήση αυτών, σε εφαρμογές. Για παράδειγμα, ο διαδικτυακός νόμος περί απορρήτου της Καλιφόρνιας, που τροποποιήθηκε τελευταία το 2013, απαιτεί από τους προγραμματιστές να έχουν πολιτικές απορρήτου που δηλώνουν εάν τρίτα μέρη μπορούν να συλλέγουν προσωπικά αναγνωρίσιμες πληροφορίες για τους χρήστες. Το 2013, η Ομοσπονδιακή Επιτροπή Εμπορίου (FTC) ακολούθησε την Goldenshore Technologies, LLC για παραβίαση του νόμου της Ομοσπονδιακής Επιτροπής Εμπορίου, επειδή η εφαρμογή «Brightest Flashlight Free» της εταιρείας είχε πολιτική απορρήτου που δεν αντικατοπτρίζει τη χρήση προσωπικών δεδομένων της εφαρμογής, συμπεριλαμβανομένων δεδομένων τοποθεσίας, και επειδή η εφαρμογή παρουσίασε στους καταναλωτές μια ψευδή επιλογή σχετικά με την κοινή χρήση δεδομένων τοποθεσίας. Σε διεθνές επίπεδο, το 2013, η ομάδα εργασίας για την προστασία των ατόμων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα του άρθρου 29 της Ευρωπαϊκής Ένωσης, έκρινε ότι η οδηγία για την προστασία δεδομένων του 1995 και η οδηγία για την προστασία της ιδιωτικής ζωής στο ηλεκτρονικό απόρρητο ισχύουν για όλες τις εφαρμογές για κινητά ανεξάρτητα από τη χώρα προέλευσης του προγραμματιστή και ότι οι χρήστες πρέπει πρώτα να δώσουν τη συγκατάθεσή τους για να μπορέσουν να εγκαταστήσουν μια εφαρμογή ή να δώσουν πρόσβαση σε οποιεσδήποτε πληροφορίες από τη συσκευή τους και να τις στείλουν σε τρίτα μέρη (θα το αναλύσουμε και στη συνέχεια).

2.3.1 Προ-εγκατεστημένες εφαρμογές

Υπάρχουν εφαρμογές στις κινητές συσκευές που είναι προ-εγκατεστημένες (βλ. Εικόνα 2), ανάλογα με τον κάθε κατασκευαστή, και συνήθως ο απλός χρήστης δεν μπορεί να τις απ' εγκαταστήσει. Οι προ-εγκατεστημένες εφαρμογές μπορούν να υπάρχουν για τη συλλογή δεδομένων και την παρακολούθηση του χρήστη και μάλιστα χωρίς να το γνωρίζει. Επιπλέον, πολλές από τις προ-εγκατεστημένες εφαρμογές, συνδέονται με κακόβουλο λογισμικό, το οποίο αντιπροσωπεύει μια πιθανή απειλή ασφάλειας για αυτόν.



ΕΙΚΌΝΑ 2: ΆΔΕΙΑ ΤΟΠΟΘΕΣΙΑΣ ΣΤΟΝ ΚΑΙΡΟ

Κεφάλαιο 3

Εφαρμογές ιχνηλάτησης Covid-19

3.1 Εισαγωγή

Ο ιός Covid-19 ήρθε στο προσκήνιο και από ότι φαίνεται ήρθε για να μείνει, το 2019 από όπου έχει πάρει και την ονομασία του, «πιάνοντας» τους πολίτες και τις αρχές εξαπίνης για τον τρόπο μετάδοσής του και για τις επιπτώσεις που προκαλεί στην υγεία. Οι κυβερνήσεις εδώ και ένα χρόνο , από την δημιουργία της παρούσης διατριβής, έχουν προβεί σε καθολική απαγόρευση κυκλοφορίας με επιβολή προστίμων σε οιονδήποτε παραβιάσει τα μέτρα προστασίας που έχουν λάβει με σκοπό να προστατέψουν τους πολίτες από το να νοσήσουν αλλά και την εξάπλωση του ιού. Μην μπορώντας όμως οι κυβερνήσεις και η πολιτική προστασία να ελέγξουν όλον αυτόν πληθυσμό για το αν τηρεί τα μέτρα προστασίας ή όχι, για το αν έχει νοσήσει αλλά δεν το

αποκαλύπτει από φόβο προς τους συμπολίτες του αλλά και κυρίως για να ελέγξει τις επαφές των ατόμων που νόσησαν και την εξάπλωση του ιού, δημιούργησαν τις εφαρμογές ιχνηλάτησης επαφών Covid-19. Οι εφαρμογές αυτές, σε παγκόσμιο επίπεδο, [11] έχουν ως σκοπό να βοηθήσουν το ιατρικό προσωπικό να εντοπίσει το μοτίβο εξάπλωσης του ιού, την παραγωγή των γραφημάτων μετάδοσής του και την ανίχνευση της προέλευσής του. Με επαρκή γνώση του ιού, η αρμόδια Αρχή κάθε χώρας μπορεί να λάβει τα απαραίτητα μέτρα (πχ απολύμανση μιας εγκατάστασης) και τη δημιουργία κατάλληλων σχεδίων (πχ επιβολή κοινωνικής απόστασης) για την καταπολέμηση του ιού και την πρόληψη μιας μελλοντικής πανδημίας ή επιδημίας. Σε ατομικό επίπεδο, βοηθά το ιατρικό προσωπικό να ειδοποιεί τα άτομα ώστε να ενημερωθούν έγκαιρα για το αν ήρθαν σε επαφή με κάποιο επιβεβαιωμένο κρούσμα του ιού και να μείνουν σε καραντίνα ή όχι. Τέτοιου είδους εφαρμογές έχουν αναπτυχθεί από πολλούς διαφορετικούς φορείς ανά τον κόσμο. Η προσέγγιση με την οποία αναπτύσσεται η κάθε εφαρμογή καταδεικνύει και τη διαφορά προσέγγισης των διαφόρων χωρών ως προς την προστασία του θεμελιώδους δικαιώματος της προστασίας προσωπικών δεδομένων. Για παράδειγμα, σε χώρες της ΕΕ γίνεται προσπάθεια να προστατεύονται κατάλληλα τα δεδομένα των χρηστών των εφαρμογών αυτών, έτσι ώστε να μην υπάρχει ο κίνδυνος δυσμενών διακρίσεων από αποκάλυψη ευαίσθητων δεδομένων υγείας σε τρίτους.

Οι εφαρμογές αυτές διαχωρίζονται σε κεντρικοποιημένες (centralized) και αποκεντρωμένες (decentralized), βασιζόμενες στο Bluetooth Low Energy(BLE), ανάλογα με το αν υπάρχει κεντρικός διακομιστής και σε εφαρμογές Bluetooth και GPS ανάλογα με το πώς γίνεται η μετάδοση μεταξύ των κινητών συσκευών.

3.2 Υπάρχουσες εφαρμογές

Από την αρχή της εξάπλωσης του ιού, συνολικά τριάντα οχτώ χώρες μέσα στις οποίες δεν βρίσκεται η Ελλάδα, έχουν δημιουργήσει τέτοιες εφαρμογές βάσει της ταξινόμησης που έχει προαναφερθεί. Κάποιες μάλιστα έχουν δημιουργήσει όχι μόνο μία αλλά και δύο και τρεις εφαρμογές, κάποιες έχουν δημιουργήσει εφαρμογές τόσο σε android όσο και σε ios λειτουργικά συστήματα, όπως το Μπαχρέϊν με τη «BeAwareBahrain», η Κολομβία με τη «CoronaApp», η Κροατία με τη «StopCovid-19», η Ισλανδία με τη «RankingC-19», ενώ άλλες έχουν δημιουργήσει εφαρμογές σε πάνω από μία γλώσσα (στη μητρική τους και στα αγγλικά). Ενδεικτικά μπορούν να αναφερθούν ότι η Αυστραλία έχει τη «CovidSafe» από τον Απρίλιο του 2020, η Αυστρία τη

«StopCorona», η Κολομβία την «CoronaApp» , ο Καναδάς την «COVID Alert», η Γερμανία τη «Corona-Warn-App», η Ιταλία την «Immuni», η Αγγλία την «NHS-19», η Σιγκαπούρη τη «TraceTogether». Αξίζει να σημειωθεί ότι την εφαρμογή της Ιρλανδίας την «κατέβασαν» και εγκατέστησαν ένα εκατομμύριο πολίτες μέσα σε δύο μέρες. Επίσης η εφαρμογή της Κολομβίας δεν καταγράφει δεδομένα αλλά βοηθά στο να διακρίνει περιοχές που είναι θετικές στον ιό και τα άτομα που βρίσκονται σε κοντινές περιοχές με πιθανή μόλυνση του ιού. Μάλιστα το κολομβιανό κράτος παρέχει δωρεάν δεδομένα και 100 λεπτά χρόνο ομιλίας κάθε μήνα σε όποιον την εγκαθιστά. Μια ακόμη εφαρμογή που αξίζει να σημειωθεί είναι της Νέας Ζηλανδίας η «NZ Covid Tracer», την οποία και χρησιμοποιούν οι επιχειρήσεις με το να «σκανάρουν» QR codes των πελατών τους για να δουν εάν έχουν βρεθεί θετικοί στον ιό και να τους απαγορεύσουν ή όχι την είσοδο στο κτίριο τους. Άλλη μια εφαρμογή πολύ σημαντική να αναφέρουμε, είναι αυτή του Κατάρ την οποία έχει επιβάλλει το κράτος να την ενεργοποιούν οι πολίτες από τη στιγμή που φεύγουν από το σπίτι. Όταν οι πολίτες εισέρχονται σε μια επιχείρηση ή σούπερ μάρκετ θα πρέπει να δείχνουν το πράσινο σήμα της εφαρμογής, σημάδι ότι δεν νοσούν από τον ιό. Από όλες αυτές τις χώρες, μόνο η Νορβηγία σταμάτησε την εφαρμογή της με το όνομα «SmitteStop», διότι ήπια περιστατικά δεν μπορούσαν να δικαιολογήσουν τον κίνδυνο έκθεσης της προσωπικής ζωής του χρήστη.

3.3 Τεχνολογίες που χρησιμοποιούνται

Στην παρούσα ενότητα θα δούμε τις διάφορες τεχνολογίες που έχουν υιοθετηθεί σε διάφορες περιπτώσεις εφαρμογών ιχνηλάτησης κρουσμάτων Covid-19.

3.3.1 Τεχνολογία των Beacons

Το beacon ξεκίνησε το 2013 από την Apple. Πρόκειται για ένα ράδιο-σήμα το οποίο χρησιμοποιείται κατά κόρον στο μάρκετινγκ. Μέσω της τεχνολογίας του Bluetooth, τα beacons δίνουν στις εταιρείες τη δυνατότητα να συλλέγουν και να στέλνουν δεδομένα από και προς τις κινητές συσκευές με στόχο να προσελκύουν έναν υποψήφιο πελάτη. Συνήθως τοποθετείται ένας ράδιο-πομπός έξω από το κατάστημα και στέλνει beacon, τα οποία είναι συνδυασμός γραμμάτων και αριθμών με αναγνωριστικό αριθμό(ID) μοναδικό για κάθε κατάστημα, με συχνότητα περίπου του ενός δέκατου του δευτερολέπτου. Τα σήματα αυτά καταγράφουν τις προτιμήσεις του πελάτη καθώς και τη συμπεριφορά του και έχουν αξία μόνο μέσω των εφαρμογών.

3.3.2 Bluetooth Low Energy-BLE

Το Bluetooth Low Energy-BLE (βλ. Εικόνα 3), είναι μία τεχνολογία η οποία δίνει τη δυνατότητα σε δύο κινητές συσκευές όταν βρίσκονται σε κοντινή απόσταση να ανταλλάσουν αναγνωριστικά καταναλώνοντας πολύ χαμηλή ενέργεια (μπαταρία). Αυτή είναι και στην ουσία η διαφορά με το πλέον γνωστό Bluetooth. Πλέον τα IOS,Android,macOS,Linux,Windows 8-10 χρησιμοποιούν το BLE. Μια τέτοιου είδους επικοινωνία αποφεύγει την τεχνολογία του GPS ή άλλους δρομολογητές όπως το WiFi, οπότε είναι και ασφαλέστερο όσον αφορά τα συστήματα ιχνηλάτησης. Στηρίζονται στην ουσία στη χρήση ψευδωνύμων τα οποία ανταλλάσσονται μέσω αναγνωριστικών «beacons» σημάτων. Όλα τα ψευδώνυμα που ανταλλάσσονται μεταξύ των κινητών συσκευών αποθηκεύονται τοπικά. Έτσι λοιπόν μια κινητή συσκευή διαθέτει μια βάση δεδομένων για τα ψευδώνυμα που εστάλησαν και μια βάση δεδομένων για αυτά που λήφθηκαν. Η κεντρική ιδέα που βασίζεται σε αυτήν την τεχνολογία, όταν χρησιμοποιείται για ιχνηλάτηση επαφών Covid-19, είναι ότι όταν ένα άτομο νοσήσει από τον ιό, οι συσκευές και επομένως οι χρήστες να ειδοποιηθούν ότι βρέθηκαν κοντά σε επιβεβαιωμένο κρούσμα αφού πρώτα έχει υπολογιστεί ένα σκορ κινδύνου (ανάλογα δηλαδή με το πόσο κοντά και για πόση ώρα έχουν έλθει κοντά, οι δύο συσκευές). Πάνω σε αυτό το σύστημα έχουν στηριχτεί κάποιες προτάσεις όπως το DP-3T,MIT-PACT,UW PACT,Apple/Google(αποκεντρωμένα συστήματα) σύστημα,PEPP-PT-NTK,PEPP-PT ROBERT(κεντρικοποιημένα συστήματα) τα οποία και θα αναλύσουμε στη συνέχεια.

ΕΙΚΌΝΑ 3: ΤΟ ΛΟΓΟΤΥΠΟ BLE

3.3.3 Ιχνηλάτηση μέσω παρακολούθησης τοποθεσίας

Τα συστήματα ιχνηλάτησης που στηρίζονται στο GPS ή στους πύργους τηλεφωνίας , λαμβάνουν περιοδικά την τοποθεσία του χρήστη και την ώρα που βρισκόταν σε αυτή την τοποθεσία. Δίνουν την ευχέρεια στις υγειονομικές αρχές να αναλύουν τις γεωγραφικές περιοχές που έχουν μολυνθεί και να ενεργούν ανάλογα με αυτές. Για παράδειγμα θα μπορούσε η εφαρμογή να προειδοποιεί το χρήστη ότι πρόκειται να εισέλθει σε περιοχή που είναι μολυσμένη και να του επιστήσει την προσοχή ή να τον ενημερώσει ότι εισέρχεται σε μία καφετέρια στην οποία είχαν εισέλθει πριν από κάποια ώρα άτομα που έχουν νοσήσει, αποτρέποντάς τον από το να μπει μέσα. Παρά τα όσα πλεονεκτήματα έχει ένα τέτοιο σύστημα , αποκαλύπτει την τοποθεσία του χρήστη που είναι μία αρκετά «επεμβατική» επεξεργασία προσωπικών δεδομένων, και η οποία εγείρει αμφιβολίες ως προς την εκπλήρωση των προϋποθέσεων νομιμότητας της επεξεργασίας προσωπικών δεδομένων. Ένα άλλο μειονέκτημα που έχει αυτό το σύστημα είναι το γεγονός ότι το GPS δεν δουλεύει καλά σε κάποιες περιοχές που έχουν ψηλά κτίρια και πυκνή βλάστηση.

Σε κάθε περίπτωση για να λειτουργήσει ένα τέτοιο σύστημα πρέπει να στηρίζεται στην αυθεντικότητα και στην εμπιστευτικότητα. Η αυθεντικότητα αναφέρεται στη σωστή μέτρηση της απόστασης μεταξύ ενός μολυσμένου ατόμου και ενός υγιούς και αυτό γιατί σύμφωνα με τα τωρινά δεδομένα για να νοσήσει κάποιος πρέπει να βρίσκεται σε απόσταση μικρότερη των 2 μέτρων, ενώ το GPS μπορεί να έχει απόκλιση έως και 5 μέτρα για τους λόγους που προαναφέραμε. Επίσης εάν κάποιο άτομο μένει σε ένα διπλανό διαμέρισμα ενός μολυσμένου ατόμου, σύμφωνα με το GPS, βρίσκονται πολύ κοντά μεταξύ τους κάτι όμως που δεν σημαίνει ότι το άτομο αυτό θα νοσήσει, μιας και πρακτικά μεταξύ τους παρεμβάλλεται ολόκληρος τοίχος και πολλά δωμάτια. Περαιτέρω, τα δεδομένα της απόστασης μπορεί να τα εκμεταλλευτεί ο οποιοσδήποτε και να τα χρησιμοποιήσει για δικό του όφελος. Εάν για κάποιο λόγο πληγεί η αυθεντικότητα, τότε αυτό μπορεί να προκαλέσει μεγάλο πανικό στον κόσμο σε περιόδους επιδημίας και πανδημίας. Η εμπιστευτικότητα, αναφέρεται στην αποκάλυψη προσωπικών δεδομένων. Τα άτομα που νοσούν δεν θα θέλουν να αποκαλύψουν την τοποθεσία τους σε κανέναν εκτός από τις υγειονομικές αρχές ώστε να αποφύγουν την ενδεχόμενη γενική κατακραυγή και τον κοινωνικό διαχωρισμό από τους υπόλοιπους. Παραδείγματα τέτοιων εφαρμογών είναι τα MIT's SafePaths, Cyprus CovTracer, Israel's Hamagen, India's Aarogya Setu.

3.4 Κεντρικοποιημένες, μη κεντρικοποιημένες και υβριδικές προσεγγίσεις

Τα συστήματα ιχνηλάτησης που είναι βασισμένα στην τεχνολογία BLE, στηρίζονται σε έναν κεντρικό διακομιστή ο οποίος αναλαμβάνει να φέρει εις πέρας κάποιες λειτουργίες. Εάν ο κεντρικός διακομιστής αναλαμβάνει όλες τις διαδικασίες ιχνηλάτησης, αναφερόμαστε σε μια κεντρικοποιημένη υλοποίηση ενώ αν τις λειτουργίες ιχνηλάτησης τις αναλαμβάνουν οι κινητές συσκευές, αναφερόμαστε σε ένα μη κεντρικοποιημένο (αποκεντρωμένο) σύστημα και αν είναι μοιρασμένες μεταξύ διακομιστή και κινητής συσκευής αναφερόμαστε σε ένα υβριδικό σύστημα.

3.4.1 Κεντρικοποιημένες υλοποιήσεις

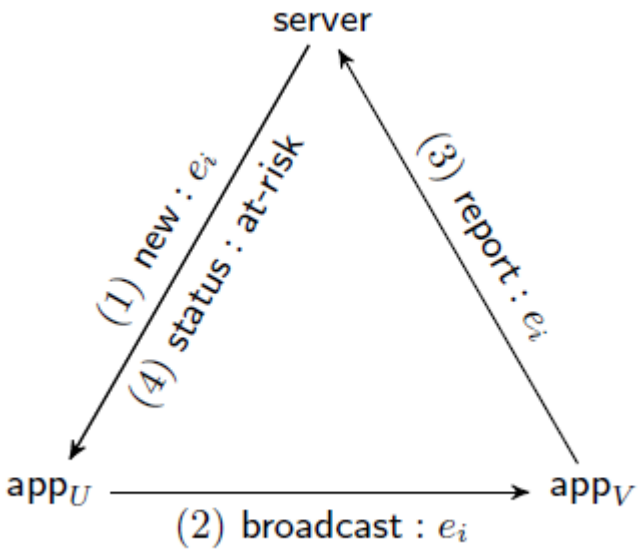
Στις κεντρικοποιημένες (centralized) εφαρμογές ιχνηλάτησης[2],[4] υπάρχει ένας κεντρικός διακομιστής στον οποίο στέλνονται όλα τα δεδομένα και βασίζεται στο Bluetooth πρωτόκολλο. Αρχικά οι χρήστες «κατεβάζουν» την εφαρμογή, την εγκαθιστούν και κάνουν εγγραφή στο διακομιστή χρησιμοποιώντας το όνομά τους, το επίθετό τους, την ηλικία τους, το τηλέφωνό τους και τον ταχυδρομικό τους κώδικα. Μετά την εγγραφή ο διακομιστής ελέγχει τον αριθμό με one time password(OTP) για να πιστοποιήσει την αυθεντικότητα του χρήστη και δημιουργεί ένα μοναδικό αναγνωριστικό (ID) για κάθε κινητή συσκευή, το οποίο είναι ένα ψευδώνυμο του χρήστη. Αφού επαληθευτεί η αυθεντικότητα του χρήστη, το ID αυτό κρυπτογραφείται με ένα μυστικό κλειδί και το αποτέλεσμα της κρυπτογράφησης (tempID) αποστέλλεται στην κινητή συσκευή του χρήστη. Τα tempID αφού κρυπτογραφούνται από τον διακομιστή, δεν αποκαλύπτουν καμία απολύτως πληροφορία για την ταυτότητα του χρήστη. Όταν δύο κινητές συσκευές με εγκατεστημένη την εφαρμογή και ανοιχτό το Bluetooth, έρθουν σε επαφή, ανταλλάσουν μηνύματα κοντινής απόστασης. Τα μηνύματα αυτά περιλαμβάνουν το tempID, το μοντέλο της συσκευής και την ισχύ μετάδοσης. Κάθε συσκευή επίσης ανιχνεύει την ισχύ του σήματος (Received Signal Strength Indicator-RSSI) και τη χρονική στιγμή παραλαβής των μηνυμάτων.

Αφού δύο κινητές συσκευές ανταλλάσουν μηνύματα κοντινής απόστασης, αυτές αμέσως θεωρούνται επαφές και αποθηκεύονται τοπικά στη συσκευή. Οι επαφές δεν αποστέλλονται στον διακομιστή παρά μόνο εάν ο χρήστης βγει θετικός και αυτό γιατί δεν υπάρχει λόγος να γεμίζει ο διακομιστής με όχι χρήσιμες πληροφορίες. Όταν οι υγειονομικές αρχές επιβεβαιώσουν ότι ο χρήστης είναι θετικός καθώς επίσης και την ταυτότητά του , τότε και μόνο τότε, τον

«σημαδεύει» ως θετικό . Το «ανέβασμα» των επαφών γίνεται με την συγκατάθεση του χρήστη και έπειτα από συνεννόηση με τον διακομιστή.

Μόλις ο διακομιστής λάβει τα μηνύματα, τα αποκρυπτογραφεί και λαμβάνει τα tempID. Με το tempID γίνεται αντιστοίχιση του χρήστη με το κινητό του τηλέφωνο. Ο διακομιστής αφού έχει λάβει τις επαφές του χρήστη τις τελευταίες 14 μέρες (σε άλλες εφαρμογές μπορεί και να ληφθεί το ιστορικό των επαφών των τελευταίων 21 ημερών), δημιουργεί ένα σκορ κινδύνου το οποίο το στέλνει στις επαφές του . Αυτό το υπολογίζει χρησιμοποιώντας την ισχύ σήματος και το σήμα για να υπολογίσει την απόσταση που βρίσκονται μεταξύ τους οι χρήστες. Με αυτό το αποτέλεσμα σε συνδυασμό με τη χρονική περίοδο που οι χρήστες ήλθαν σε επαφή, υπολογίζει το σκορ κινδύνου δηλαδή κατά πόσο πιθανό ή όχι είναι ένας χρήστης να έχει νοσήσει από τον ιό. Εάν το σκορ κινδύνου είναι πάνω από ένα όριο που έχει ορίσει η εφαρμογή, τότε ο διακομιστής ενημερώνει τον χρήστη ότι πρέπει να μείνει σε καραντίνα και εφόσον παρουσιάσει σοβαρά συμπτώματα να μπει σε νοσοκομείο και να λάβει ιατρική περίθαλψη. Εάν το σκορ είναι πολύ μικρό, τότε τον ενημερώνει ότι είναι ασφαλής και ότι δεν έχει νοσήσει από τον ιό.

Πώς όμως πρακτικά λειτουργεί μια τέτοια διαδικασία; Η εφαρμογή ενός χρήστη ‘U’[4], διαθέτει δύο λίστες από αναγνωριστικά. Η μία λίστα είναι εκείνη με τα αναγνωριστικά που θα στείλει (έστω Lout) και η άλλη είναι η λίστα με τα αναγνωριστικά που θα λάβει (έστω Lin). Σε κάθε περίοδο χρόνου, η οποία εξαρτάται από την εφαρμογή, η κινητή συσκευή στέλνει σε άλλες που βρίσκονται κοντά της, εφήμερα αναγνωριστικά(ephemeral identifiers) e_i και ταυτόχρονα λαμβάνει e_j από άλλους χρήστες. Η εφαρμογή μετά το πέρασμα κάποιου χρονικού διαστήματος το οποίο εξαρτάται από την εφαρμογή και είναι σίγουρα πάνω από 14 μέρες απορρίπτει παλιά αναγνωριστικά. Το Lout στα κεντρικοποιημένα συστήματα λαμβάνεται από τον διακομιστή (βλ. Εικόνα 4). Όταν κάποιος χρήστης νοσήσει και αποφασίσει οικειοθελώς να το κοινοποιήσει στον διακομιστή, επικοινωνεί με την Αρχή υγείας της χώρας του, η οποία πιστοποιεί την αυθεντικότητά του στέλνοντας του έναν κωδικό ώστε να μπορεί να ανεβάσει την πληροφορία της ασθένειάς του στον κεντρικό διακομιστή. Αυτό που στην ουσία στέλνει στον διακομιστή ο χρήστης, είναι η Lin λίστα με τα αναγνωριστικά.

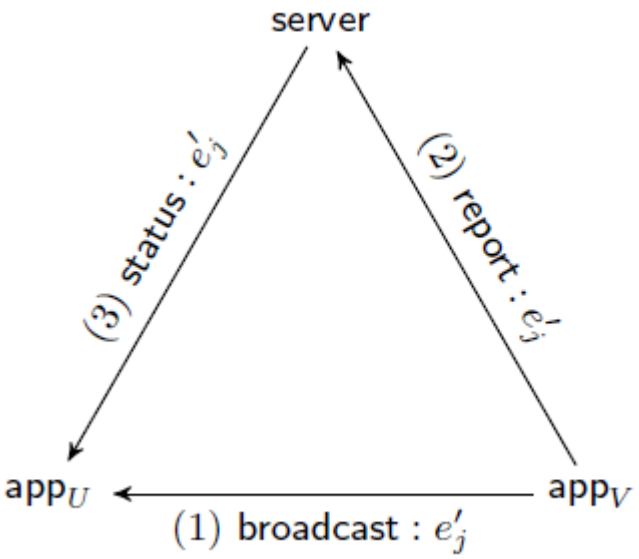


ΕΙΚΌΝΑ 4: ΚΕΝΤΡΙΚΟΠΟΙΗΜΕΝΟ ΣΥΣΤΗΜΑ [4]

Συνοψίζοντας , ο διακομιστής έχει μεγάλο ρόλο στα κεντρικοποιημένα συστήματα γιατί είναι αυτός που πρέπει να αυθεντικοποιήσει τον χρήστη, να δημιουργήσει τα εφήμερα αναγνωριστικά , να δημιουργήσει το σκορ κινδύνου και να ενημερώσει τις κοντινές επαφές του εφόσον το σκορ κινδύνου έχει ξεπεράσει ένα ορισμένο, από την εφαρμογή, όριο. Ο διακομιστής σε αυτό το σύστημα θα πρέπει να θεωρείται έμπιστος διότι εγείρονται θέματα ιδιωτικότητας, στα οποία θα αναφερθούμε και στη συνέχεια.

3.4.2 Αποκεντρωμένες Υλοποιήσεις

Οι αποκεντρωμένες (decentralized)εφαρμογές, είναι οι εφαρμογές [2],[4]οι οποίες βασίζονται και αυτές στο πρωτόκολλο του Bluetooth αλλά σε αυτές ο διακομιστής έχει πολύ μικρό ρόλο αφού όλες οι διαδικασίες και οι υπολογισμοί γίνονται τοπικά στην κινητή συσκευή του χρήστη. Αρχικά ο χρήστης «κατεβάζει» την εφαρμογή η οποία ενεργοποιεί το Bluetooth του και πιστοποιεί την αυθεντικότητα του χρήστη με το τηλέφωνό του. Βέβαια υπάρχουν και αποκεντρωμένες εφαρμογές που δεν απαιτούν εγγραφή του χρήστη στον διακομιστή.



ΕΙΚΟΝΑ 5: ΑΠΟΚΕΝΤΡΩΜΕΝΟ ΣΥΣΤΗΜΑ[4]

Μόλις εγκατασταθεί η εφαρμογή, η κινητή συσκευή του χρήστη δημιουργεί ένα αναγνωριστικό (e_i) το οποίο λήγει σε ένα διάστημα που έχει οριστεί (για παράδειγμα μιας ώρας) και το αποθηκεύει στη λίστα Lout (βλ Εικόνα 5). Στη συνέχεια αυτό το αναγνωριστικό καθώς επίσης η χρονική στιγμή που δημιουργήθηκε, χρησιμοποιούνται σε μία ψευδο-τυχαία συνάρτηση για να δημιουργηθεί το αναγνωριστικό το οποίο θεωρείται «ανώνυμο» αφού δεν μπορεί να συνδεθεί με το κινητό ή την ταυτότητα του χρήστη. Η εφαρμογή δημιουργεί συνεχώς αναγνωριστικά τα οποία και μεταδίδει μέσω του BLE σε άλλες κοντινές συσκευές οι οποίες με τη σειρά τους, αποθηκεύουν τα αναγνωριστικά που έλαβαν τοπικά στη συσκευή τους(Lin). Οι εφαρμογές αυτό που στην ουσία αποθηκεύουν είναι το αναγνωριστικό, η χρονική στιγμή που δημιουργήθηκε καθώς επίσης και τη μέγιστη ισχύ του σήματος (RSSI). Όταν η εφαρμογή λάβει ίδια αναγνωριστικά μέσα σε ένα διάστημα ενός λεπτού, τα απορρίπτει. Εάν ένας χρήστης νοσήσει και ζητήσει από την Αρχή υγείας του εκάστοτε κράτους του, την άδεια (αποστέλλοντας του έναν κωδικό που πιστοποιεί την αυθεντικότητά του), «ανεβάζει» οικειοθελώς, όλα τα αναγνωριστικά που έχει αποθηκευμένα η συσκευή του στον διακομιστή, τη χρονική στιγμή που δημιουργήθηκαν καθώς και την ημερομηνία λήξης τους. Κάθε μέρα η εφαρμογή επικοινωνεί με τον διακομιστή για να «κατεβάσει» τοπικά όλα τα αναγνωριστικά που έχουν ανεβάσει τα άτομα που νόσησαν. Μόλις τα λάβει, ψάχνει να βρει μέσα στη βάση δεδομένων της αν υπάρχουν ίδια αναγνωριστικά με αυτά που «κατέβασε» και που αυτό θα σήμαινε ότι έχει έρθει σε επαφή με επιβεβαιωμένο κρούσμα. Αν όντως υπάρχουν στη βάση της τέτοια αναγνωριστικά, παράγεται μέσω συνάρτησης, βασισμένης στη χρονική στιγμή του αναγνωριστικού και στην ισχύς του

σήματος, η εγγύτητα των δύο συσκευών καθώς επίσης και η χρονική διάρκεια που διήρκησε ώστε να δημιουργηθεί το σκορ κινδύνου του χρήστη (το πόσο πιθανό δηλαδή είναι αυτός να έχει όντως νοσήσει).

Συνοψίζοντας λοιπόν, στα αποκεντρωμένα συστήματα, το βασικό ρόλο τον έχει η εφαρμογή και όχι ο διακομιστής, όπως μελετήσαμε προηγουμένως στα κεντρικοποιημένα συστήματα. Η εφαρμογή είναι αυτή που δημιουργεί τα αναγνωριστικά, τα εκπέμπει μέσω BLE και αποθηκεύει τοπικά όσα έλαβε από άλλες συσκευές. Και είναι εκείνη που δημιουργεί το σκορ κινδύνου του χρήστη της τον οποίο και ενημερώνει ανάλογα. Ο ρόλος του διακομιστή είναι να αποθηκεύει τα αναγνωριστικά μόνο των χρηστών που νόσησαν, τα οποία και κατεβάζει η εφαρμογή ανά τακτά χρονικά διαστήματα για να τα συγκρίνει με αυτά που είναι αποθηκευμένα στη βάση της.

3.4.3 Υβριδικές Υλοποιήσεις

Στα υβριδικά συστήματα [2], ο χρήστης «κατεβάζει» την εφαρμογή, την εγκαθιστά και ενεργοποιεί το BLE του. Στη συνέχεια κάνει εγγραφή στον διακομιστή ο οποίος πιστοποιεί τον χρήστη με OTP στο τηλέφωνό του και την εφαρμογή με διακριτικό πρόσβασης που εξέδωσε ο ίδιος. Στη συνέχεια ο διακομιστής διαγράφει το τηλέφωνο του χρήστη, δημιουργεί ένα κρυπτογραφημένο κλειδί που το στέλνει στην εφαρμογή και το διαγράφει από τη βάση του. Έπειτα η εφαρμογή δημιουργεί ένα εφήμερο αναγνωριστικό (EphID=g^a) χρησιμοποιώντας τον αλγόριθμο Diffie Hellman το οποίο είναι έγκυρο για 15 λεπτά και αρχίζει να το μεταδίδει μέσω BLE. Μόλις μια κοντινή συσκευή λάβει το εφήμερο αναγνωριστικό, η εφαρμογή δημιουργεί δύο ιδιωτικά διακριτικά εγγύτητας (PET) όπου το PET1 είναι αποτέλεσμα συνάρτησης κατακερματισμού (hash function) και ισούται με PET1=H('1'|($g^{(a,b)}$) αποθηκεύεται στη βάση δεδομένων που αναζητάει δεδομένα και το PET2=(H'2'|$g^{(a,b)}$) το οποίο μαζί με το χρόνο και τη διάρκεια εγγύτητας αποθηκεύεται στη βάση δεδομένων που ανεβάζει στον διακομιστή.

Μόλις ένας χρήστης νοσήσει από τον ιό, ανεβάζει στη βάση δεδομένων το αναγνωριστικό , το κρυπτογραφημένο κλειδί που του είχε στείλει ο διακομιστής, το PET, το χρόνο και τη διάρκεια εγγύτητας και υπολογίζει το σκορ κινδύνου του.

Οι χρήστες για να δουν εάν έχουν νοσήσει, «ανεβάζουν» το PET στη βάση δεδομένων του διακομιστή μέσω ανώνυμου καναλιού και εκείνος συγκρίνει τα PET που έλαβε από τους χρήστες που «ρωτάνε» με τα PET των χρηστών που νόσησαν και χρησιμοποιώντας τη διάρκεια και το

χρόνο εγγύτητας υπολογίζει το σκορ κινδύνου και τους ειδοποιεί εάν πρέπει ή όχι να μείνουν σε καραντίνα.

Συνοψίζοντας, το υβριδικό σύστημα προσπαθεί να «μοιράσει» τις λειτουργίες μεταξύ του διακομιστή και της εφαρμογής κυρίως για λόγους ασφαλείας, όπως θα δούμε και παρακάτω, και αυτός είναι ο κύριος λόγος που ο διακομιστής διαγράφει το τηλέφωνο του χρήστη μετά την πιστοποίηση της αυθεντικότητάς του .Ο λόγος που σε ένα τέτοιο σύστημα το σκορ κινδύνου το αναλαμβάνει ο διακομιστής είναι διότι οι υγειονομικές αρχές θέλουν να γνωρίζουν ποιες περιοχές είναι επικίνδυνες λόγω μόλυνσης και για να κάνουν καλύτερη ιχνηλάτηση των επαφών των ατόμων που νόσησαν.

3.5 Decentralized Privacy-Preserving Proximity Tracing (DP-3T)

Το σύστημα Αποκεντρωμένης Προστασίας Προσωπικών Δεδομένων (DP-3T) [9] στηρίζεται στη δημιουργία εφήμερων ψευδωνύμων τα οποία στέλνονται μέσω BLE και τα οποία δημιουργούνται από μυστικά κλειδιά τα οποία τα διαχειρίζεται η κινητή συσκευή και όχι ο διακομιστής. Μιας και ανήκει στα αποκεντρωμένα συστήματα, δεν απαιτείται εγγραφή του χρήστη και ο καθένας μπορεί να το χρησιμοποιεί με το να δημιουργεί ένα μυστικό συμμετρικό κλειδί (έστω SKt όπου t η μέρα που δημιουργήθηκε). Κάθε μυστικό κλειδί είναι έγκυρο για μία μέρα και το επόμενο κλειδί είναι αποτέλεσμα συνάρτησης κατακερματισμού (hash function) του αρχικού κλειδιού, δηλαδή $SK_{t+1}=H(SK_t)$. Η κινητή συσκευή δημιουργεί μία σειρά από n εφήμερα αναγνωριστικά (EphID) για μία περίοδο, που έχει ορίσει το πρωτόκολλο και που συνήθως είναι ένα λεπτό, τα οποία είναι της μορφής : $EphID_1||EphID_n=PRG(PRF(SK_t,"broadcast\ key"))$ όπου PRG είναι ένας κρυπτογραφικός αλγόριθμος ροής (stream cipher) και η PRF είναι μία ψευδό-τυχαία συνάρτηση. Τα EphID έχουν μέγεθος 128 bits και συνεχώς μεταδίδονται σε τυχαία σειρά ανά διαστήματα κάποιων «l» λεπτών σε κοντινούς χρήστες οι οποίοι χρησιμοποιώντας τα EphID , τη μέρα και τη μέτρηση της απόστασης μεταξύ τους, δημιουργούν ένα ιστορικό εγγύτητας. Όταν κάποιος χρήστης βγει θετικός στον ιό, ανεβάζει στον διακομιστή το μυστικό κλειδί και τη μέρα $(SK_{t0},t0)$ κι εκείνος με τη σειρά του το προωθεί στους υπόλοιπους χρήστες. Οι χρήστες μόλις λάβουν το ζευγάρι $(SK_{t0},t0)$ από τον διακομιστή, δημιουργούν όλα τα εφήμερα αναγνωριστικά (EphID) εκείνης της μέρας(t0) και ελέγχουν αν ταιριάζουν με τα αναγνωριστικά που έχουν αποθηκευμένα στη συσκευή. Αν ταιριάζουν, η εφαρμογή υπολογίζει ένα σκορ κινδύνου του χρήστη, βάσει του αριθμού των λεπτών που έχουν εκτεθεί με τα συγκεκριμένα αναγνωριστικά

και αυτό γιατί τα εφήμερα αναγνωριστικά είναι έγκυρα σε διάστημα ενός λεπτού. Οι χρήστες που έχουν έρθει σε επαφή με επιβεβαιωμένο κρούσμα και είτε έκαναν τεστ και βγήκαν θετικοί είτε όχι και μένουν σε καραντίνα, μπορούν εθελοντικά να ανεβάσουν τον αριθμό των εφήμερων αναγνωριστικών για τις τελευταίες 14 ημέρες. Το DP-3T σύστημα προστατεύει τα προσωπικά δεδομένα των χρηστών μιας και τα εφήμερα αναγνωριστικά δεν αποκαλύπτουν ούτε την τοποθεσία ούτε το χρόνο ούτε τα άτομα που εκτέθηκαν.

3.6 Google/Apple Exposure Notification (GAEN)

Τον Απρίλιο του 2020 η Google και η Apple [13] συνεργάστηκαν για να δημιουργήσουν μια υπηρεσία ειδοποίησης έκθεσης στον ιό Covid-19, βασισμένη στο BLE πρωτόκολλο. Η υπηρεσία αυτή, αρχικά γνωστή ως έργο παρακολούθησης επαφών προστασίας προσωπικών δεδομένων, ονομάστηκε GAEN (Google/Apple Exposure Notification) και είναι αυτή που διαχειρίζεται την αποστολή και τη λήψη BLE beacons και καταγράφει τη διάρκεια και τη ισχύ του σήματος των ληφθέντων beacons. Σε Android συσκευές, προστέθηκε σε αυτές μέσω ενημέρωσης των Υπηρεσιών της Google Play, υποστηρίζοντας όλες τις εκδόσεις από το Android Marshmallow και μετά. Το GAEN είναι ένα αποκεντρωμένο πρωτόκολλο και χρησιμοποιείται ως δυνατότητα συμμετοχής σε εφαρμογές ιχνηλάτησης COVID-19 που αναπτύχθηκαν και δημοσιεύθηκαν από εξουσιοδοτημένες υγειονομικές αρχές. Είναι παρόμοιο με το πρωτόκολλο Αποκεντρωμένης Προστασίας Προσωπικών Δεδομένων (DP-3T) και έχει σχεδιαστεί για να διατηρεί τη διαλειτουργικότητα μεταξύ συσκευών Android και iOS, οι οποίες αποτελούν την απόλυτη πλειοψηφία της αγοράς.

Όλες οι εφαρμογές που είναι βασισμένες στο GAEN χωρίζονται σε δύο τμήματα. Το πρώτο είναι η εφαρμογή του χρήστη την οποία διαχειρίζονται οι υγειονομικές Αρχές και αποτελεί τη διεπαφή του χρήστη και το δεύτερο είναι το τμήμα των εφαρμογών που αποτελούν μέρος του Google Play Services οι οποίες διαχειρίζονται από την Google. Η εφαρμογή είναι εκείνη που αλληλεπιδρά με τον διακομιστή για να «ανεβάσει» τα «διαγνωστικά κλειδιά» όταν κάποιος βγει θετικός , να «κατεβάσει» τα δημόσια κλειδιά για να ελέγξει αν ο χρήστης έχει έρθει σε επαφή με θετικά διαγνωσμένο άτομο και για να «κατεβάσει» ενημερώσεις.

Ποια είναι λοιπόν τα δεδομένα που «διαχειρίζεται» το GAEN;

- Τα Bluetooth αναγνωριστικά και τα δεδομένα εγγύτητας τα οποία αποθηκεύονται τοπικά στις συσκευές του χρήστη

- Το αποτέλεσμα θετικού διαγνωστικού τεστ το οποίο το ανεβάζει ο χρήστης μέσω της εφαρμογής στον διακομιστή μαζί με τα αναγνωριστικά εγγύτητας των επαφών του

- Συσχετιζόμενη πληροφορία: όταν κάποιος χρήστης ειδοποιηθεί ότι έχει εκτεθεί στον ιό μέσω της εφαρμογής, η IP διεύθυνσή τους και άλλα μεταδεδομένα θα είναι ανιχνεύσιμα από τον διακομιστή. Βέβαια η Apple/Google απαιτούν, αυτή τη χρονική στιγμή, από όλες τις εφαρμογές που χρησιμοποιούν το GAEN να μην συλλέξουν και να μην διατηρήσουν αυτές τις πληροφορίες.

- Ειδοποιήσεις σε εκτεθειμένους χρήστες. Το GAEN θα κατεβάσει και θα μεταδώσει τα αναγνωριστικά θετικών διαγνωσμένων χρηστών μία φορά την ημέρα και στη συνέχεια θα συσχετίσει τα τηλέφωνα με τα αναγνωριστικά αυτά ώστε χρησιμοποιώντας κάποιον αλγόριθμο να αξιολογήσει τον κίνδυνο έκθεσης για τον χρήστη του.

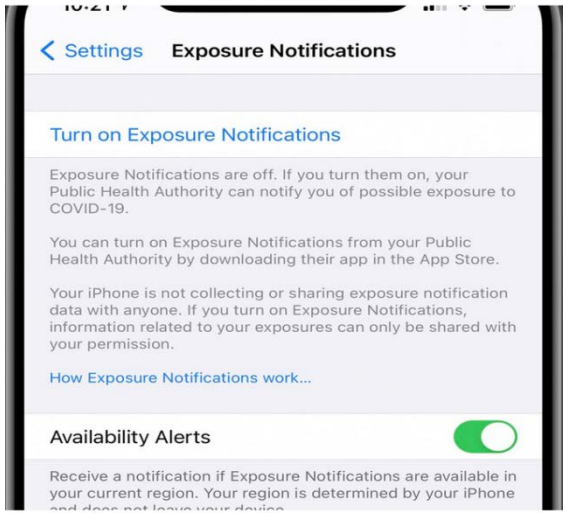
- Δεδομένα έκθεσης που συλλέγονται από τις εφαρμογές που χρησιμοποιούν το GAEN με δεδομένα τοποθεσίας του χρήστη προκειμένου να βοηθήσουν τις αρχές ώστε (i) να διασφαλίσουν την καραντίνα των μολυσμένων και εκτεθειμένων ατόμων,(ii) να χρησιμοποιηθούν αθροιστικά με άλλα δεδομένα για να παρακολουθούν την εξάπλωση του ιού σε έναν πληθυσμό και (iii) να τα ανακοινώσει σε τρίτες οντότητες, όπως οι εργοδότες, δίνοντάς τους το «πράσινο φως» για τους εργαζομένους τους ότι είναι καθαροί.

Οι υπηρεσίες της google play των εφαρμογών ιχνηλάτησης φέρεται να έχουν ευπάθειες όσον αφορά την προστασία της ιδιωτικότητας των χρηστών [5]. Οι υπηρεσίες της google play συνδέονται με τους διακομιστές της google κάθε είκοσι λεπτά με αποτέλεσμα να αποκαλύπτουν τη IP διεύθυνση του χρήστη, την τοποθεσία του και να δίνεται η ευκαιρία σε αναγνωριστικά από την ίδια συσκευή να συνδεθούν μεταξύ τους. Η google τονίζει ότι χρησιμοποιεί τις διευθύνσεις για να υπολογίσει την τοποθεσία, όμως δεν είναι σαφές για ποιες εφαρμογές χρησιμοποιούνται αυτές οι διευθύνσεις. Ακόμα, όταν η επιλογή «χρήση και διαγνωστικά» είναι επιλεγμένη στις υπηρεσίες της google play, κάτι που είναι προεπιλεγμένο, τότε τα δεδομένα τηλεμετρίας της GAEN αποκαλύπτονται στη google. Άλλα δεδομένα που στέλνουν οι υπηρεσίες της google play στην google είναι το IMEI του τηλεφώνου, ο σειριακός αριθμός της κάρτας sim, η ηλεκτρονική διεύθυνση του χρήστη και η MAC διεύθυνση του WiFi του. Στα διάφορα τεστ που έγιναν σε πρόσφατη έρευνα στο [5] ακόμα κι αν απενεργοποίησαν όλες τις εφαρμογές της google και

άφησαν μόνο το GAEN, οι εφαρμογές ιχνηλάτησης συνέχισαν να στέλνουν δεδομένα στην google με αποτέλεσμα να τίθεται εν αμφιβόλω η συμμόρφωση της εφαρμογής με το νομικό πλαίσιο προστασίας προσωπικών δεδομένων. Αυτό που προτείνεται είναι να ενημερώνουν γραπτώς τους χρήστες ότι και μόνο που χρησιμοποιούν τις υπηρεσίες της google play υπάρχουν προσωπικά τους δεδομένα που στέλνονται στη google, να δίνεται η δυνατότητα στους χρήστες να απενεργοποιούν τις υπηρεσίες της google play οι οποίες είναι προ εγκατεστημένες στις συσκευές τους και οι κυβερνήσεις που στηρίζουν τις εφαρμογές ιχνηλάτησης τους στο GAEN, να επανεξετάσουν την ιδιωτικότητα των δεδομένων των χρηστών.

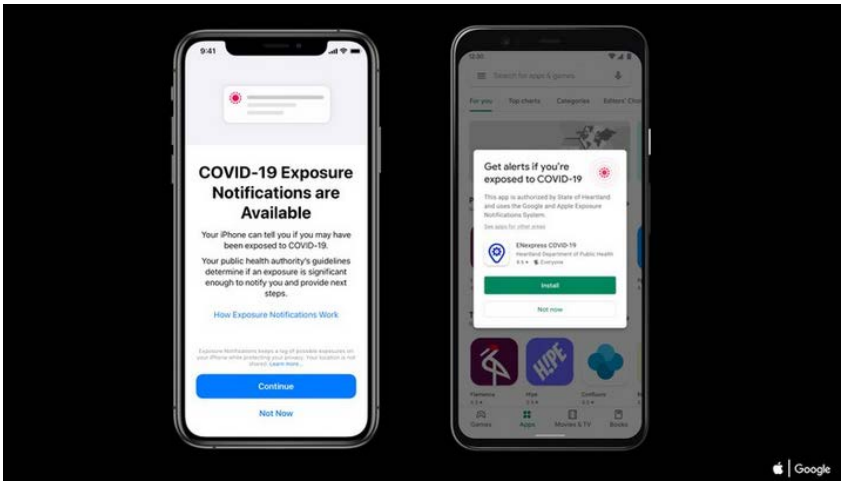
Δύο εφαρμογές που στηρίζονται σε υπηρεσίες του GAEN [5]είναι η ProteGo Safe της Πολωνίας και η Apturi Covid της Λετονίας. Η πρώτη χρησιμοποιεί την google Firebase η οποία είναι μια πλατφόρμα που αναπτύχθηκε από την Google για να μεταφέρει ρυθμίσεις διαμόρφωσης και την υπηρεσία google's Safety Net για να πιστοποιήσει την αυθεντικότητα της εφαρμογής. Όμως χρησιμοποιώντας δυο υπηρεσίες της google για την εν λόγω διαχείριση, εκτίθενται τα προσωπικά δεδομένα του χρήστη. Η δεύτερη εφαρμογή χρησιμοποιεί το Firebase για να ελέγχει τις αντιδράσεις των χρηστών με την εφαρμογή, κάτι το οποίο δεν χρειάζεται να αποκαλύπτεται στη google. Πρέπει να δίνεται η δυνατότητα στους χρήστες να απενεργοποιούν αυτή τη δυνατότητα.

Το GAEN όπως προαναφέρθηκε, είναι προ εγκατεστημένο στις κινητές συσκευές και ο χρήστης μπορεί να το ενεργοποιήσει ή να το απενεργοποιήσει όποτε το θελήσει. Εάν το GAEN υπάρχει στη χώρα του χρήστη, τότε του δίνει τη δυνατότητα να το ενεργοποιήσει από τις ρυθμίσεις της κινητής συσκευής, όπως φαίνεται και στην εικόνα 6.



ΕΙΚΌΝΑ 6: ΟΘΟΝΗ ΡΥΘΜΙΣΕΩΝ ΣΤΟ GAEN

Άλλες χώρες που χρησιμοποιούν το GAEN είναι η Σουηδία, η Ιταλία, η Γερμανία, η Σαουδική Αραβία, η Ιρλανδία, η Σκωτία, η Αγγλία και στην Αμερική η Βιρτζίνια, η Βόρεια Ντακότα, η Αριζόνα, η Νεβάδα, το Κολοράντο, οι οποίες είτε χρησιμοποιούν εφαρμογές βασισμένες στο GAENείτε εκμεταλλεύονται την υπηρεσία που δίνει η google/apple να χρησιμοποιούν την ειδοποίηση έκθεσης χωρίς τις εφαρμογές (βλ Εικόνα 7).



ΕΙΚΌΝΑ 7: ΕΝΕΡΓΟΠΟΙΗΣΗ ΤΟΥ GAEN

3.7 Pan-European Privacy Preserving Proximity Tracing (PePP-PT)

Το PePP-PT [9] είναι ένα πανευρωπαϊκό σύστημα ιχνηλάτησης επαφών βασισμένο στο κεντρικοποιημένο σύστημα χρησιμοποιώντας το BLE. Όπως σε όλα τα κεντρικοποιημένα συστήματα, υπάρχει ένας κεντρικός διακομιστής τον οποίο ελέγχουν οι υγειονομικές αρχές της εκάστοτε χώρας. Ο διακομιστής, παράγει και στη συνέχεια μεταδίδει κρυπτογραφημένα ψευδώνυμα στην κινητή συσκευή του χρήστη. Μόλις ένας χρήστης νοσήσει, μπορεί να στείλει όλα τα συλλεγόμενα ψευδώνυμα των τελευταίων 14^{ων} ημερών στον διακομιστή ο οποίος τα αποκρυπτογραφεί για να φτιάξει το σκορ κινδύνου των επαφών του και να τους ειδοποιήσει. Το PePP-PT στόχο έχει να παρέχει ιχνηλάτηση σε όλους τους χρήστες ανεξαρτήτως της Ευρωπαϊκής χώρας που ζουν. Υπάρχουν δύο υλοποιήσεις του συστήματος PePP-PT, η PePP-PT NTK και η ROBERT οι οποίες διαφέρουν σε πολύ μικρές λεπτομέρειες.

3.7.1 PePP-PT NTK

Στο PePP-PT NTK [9]στηρίζεται η γερμανική εφαρμογή ιχνηλάτησης. Αφού ο χρήστης εισέλθει στο σύστημα, δημιουργείται στον διακομιστή τυχαία ένα ψευδώνυμο μεγέθους 128 bit το λεγόμενο «persistent user identification»(PUID). Στη συνέχεια, η εφαρμογή ζητά από τον διακομιστή μια λίστα από μικρής διάρκειας ζωής ψευδωνύμων, τα λεγόμενα EBID. Το EBID δημιουργείται με το να κρυπτογραφηθεί το PUID με ένα κλειδί BK_t το οποίο είναι αποθηκευμένο και γνωστό μόνο στον διακομιστή και νόμιμο για ορισμένο χρονικό διάστημα t. Έτσι λοιπόν έχουμε $EBID_t$= EncAES(BK_t,PUID). Στη συνέχεια η εφαρμογή διαλέγει το EBID το οποίο είναι έγκυρο για τον χρόνο t και αρχίζει να το μεταδίδει και ταυτόχρονα «σκανάρει» για EBID από άλλες συσκευές που βρίσκονται κοντά και τα αποθηκεύει τοπικά στη συσκευή μαζί με το χρόνο t_s και τα μεταδεδομένα btdata του καναλιού του Bluetooth. Τα μεταδεδομένα περιλαμβάνουν το σήμα μετάδοσης και το σήμα λήψης. Η τριπλέτα t_s, btdata, EBID, ονομάζεται δεδομένα εγγύτητας επαφής (Contact Data Time- CDT) την οποία και διατηρεί για 21 ημέρες. Όταν κάποιος χρήστης νοσήσει, «σκανάρει» το barcode του τεστ που έχει κάνει από πιστοποιημένο διαγνωστικό κέντρο και έχει τη δυνατότητα να ανεβάσει στον διακομιστή το CDT. Μόλις εκείνος το παραλάβει, το αποκρυπτογραφεί χρησιμοποιώντας το κλειδί BK_t που είναι νόμιμο για τον συγκεκριμένο χρήστη και λαμβάνει το PUID: PUID=DecAES(BK_t ,$EBID_t$). Τα btdata τα χρησιμοποιεί για να δημιουργήσει το σκορ κινδύνου για τις επαφές του, υπολογίζοντας την απόσταση του χρήστη με την εκάστοτε επαφή του και αν κάποια επαφή θεωρηθεί ότι βρίσκεται σε μεγάλο κίνδυνο μόλυνσης να την ειδοποιήσει.

3.7.2 Προσέγγιση ROBERT

Η ROBERT [9] χρησιμοποιεί 3DES κρυπτογράφηση αντί για AES. Σε αυτό το πρωτόκολλο, αρχικά ο χρήστης εγγράφεται στον διακομιστή ο οποίος με τη σειρά του δημιουργεί ένα μοναδικό αλλά τυχαίο αναγνωριστικό ID για κάθε χρήστη X. Το ID έχει μήκος 40 bit. Στη συνέχεια δημιουργεί ένα μυστικό κλειδί K_x, το οποίο και το «μοιράζεται» με την εφαρμογή καθώς επίσης την ώρα I, την τιμή epoch_duration_sec και τη χρονική στιγμή στην οποία ξεκινάει η επόμενη ώρα. Για κάθε χρήστη λοιπόν, ο διακομιστής συχνά δημιουργεί μια τριπλέτα από ($EBID_x$,I,$ECC_{x,i}$) όπου i η χρονική διάρκεια στην οποία η τριπλέτα είναι νόμιμη και έχει μέγεθος 24 bit. Το αναγνωριστικό είναι της μορφής $EBID_x$=ENC(K_s,i|ID_x) και ως αλγόριθμος κρυπτογράφησης, όπως προαναφέρθηκε, χρησιμοποιείται ο 3DES παρέχοντας επιπλέον προστασία. Το CC_x είναι ο κωδικός της χώρας και έχει μέγεθος 8 bit, ενώ το ECC_x είναι το αποτέλεσμα της xor συνάρτησης του κωδικού της χώρας CC_x με τα 8 πιο σημαντικά bits του $EBID_x$, προσθέτοντας τον

απαραίτητο αριθμό μηδενικών και κρυπτογραφώντας με AES, δηλαδή είναι της μορφής $ECC_{x,i}$=MSB(AES(KG,$EBID_{x,i}$|0^{64})) xor CC_x (MSB=most significant bit). Η εφαρμογή συχνά στέλνει μηνύματα χαιρετισμού μέσω BLE όπου το κάθε μήνυμα 'M' περιλαμβάνει $M_{x,i}$=$ECC_{x,i}$|$EBID_{x,i}$|Time και την $MAC_{x,i}$ Η MAC υπολογίζεται με τη συνάρτηση κατακερματισμού HMAC-SHA256(Kx,c1|Mx,i).

Όταν ένας χρήστης νοσήσει, μπορεί να ανεβάσει τη λίστα επαφών του στον διακομιστή ο οποίος με τη σειρά του αποκρυπτογραφεί τα $ECC_{x,i}$, CC_x και ελέγχει αν ταιριάζει ο κωδικός με τη χώρα του. Αν δεν ταιριάζει, προωθεί τη λίστα στον διακομιστή της χώρας με κωδικό CC.Στη συνέχεια, ελέγχει εάν ο χρόνος ταιριάζει με τον χρόνο που ήταν «μολυσμένος» ο χρήστης ενώ τα παλαιότερα τα διαγράφει. Έπειτα, αποκρυπτογραφεί το $EBID_{x,i}$ για να βρει το i_x|ID_x. Ελέγχει αν ο χρόνος ταιριάζει με την εποχή i_x, υπολογίζει το K_x το οποίο είναι συνδυασμένο με το ID$_x$ και πιστοποιεί αν η $MAC_{x,i}$ είναι σωστή ελέγχοντας τη συνάρτηση κατακερματισμού $MAC_{x,i}$=HMAC-SHA256(K_x,c_1|$ECC_{x,i}$|$EBID_{x,i}$|Time). Αν ο διακομιστής ελέγξει όλα τα παραπάνω και τα βρει σωστά τότε ανανεώνει τη λίστα του χρήστη για να βρει ποια στιγμή εκείνος νόσησε. Για να ελέγξει ένας χρήστης αν νόσησε, αποστέλλει μέσω της εφαρμογής, ένα αίτημα περιλαμβάνοντας το $EBID_{x,i}$, το χρόνο και το $MAC_{x,i}$=HMAC-256(K_A,c_2|$EBID_{x,i}$|Time) στον διακομιστή (το c_2 είναι μια σταθερή τιμή). Ο διακομιστής αποκρυπτογραφεί τα $EBID_{x,I}$,Time, $MAC_{x,i}$. Και απαντάει με '1' αν ο χρήστης βρίσκεται σε κίνδυνο έκθεσης και '0' αν δεν βρίσκεται.

Συνοψίζοντας λοιπόν και οι δύο προσεγγίσεις στέλνουν μετρήσεις μέσω Bluetooth σε ένα κεντρικό διακομιστή ο οποίος δημιουργεί ένα σκορ κινδύνου προτού ειδοποιήσει τους χρήστες ότι διατρέχουν κίνδυνο έκθεσης στον ιό αντί αυτή η διαδικασία να γίνει τοπικά στην εφαρμογή του χρήστη. Καθώς λοιπόν οι συνθήκες εξάπλωσης του ιού δεν είναι ακόμα σαφείς, η εκτίμηση κινδύνου θα πρέπει συνεχώς να προσαρμόζεται στα νέα δεδομένα. Ο αλγόριθμος εκτίμησης κινδύνου έκθεσης στον ιό δεν είναι απλός, περιλαμβάνει κρυπτογραφήσεις και διάφορους υπολογισμούς κάτι που του παρέχει ασφάλεια στις εισβολές. Η "επαφή" δεν είναι απαραίτητα μια αδιάλειπτη ακολουθία εκπομπών BLE και η εκτίμηση κινδύνου πρέπει να λαμβάνει υπόψη τα κενά στις αλληλουχίες EBID, τις διαφορές στην ισχύ RSSI, TX και RX κ.λπ.

3.8 Ασφαλής υπολογισμός πολλαπλών μερών

Τα θεμέλια για τον ασφαλή υπολογισμό πολλών μερών [12](secure multi-party computation-MPC) ξεκίνησαν στα τέλη της δεκαετίας του 1970 με το έργο στο νοητικό πόκερ, το οποίο

αποτέλεσε μία κρυπτογραφική διαδικασία που προσομοιώνει παιχνίδια και υπολογιστικές εργασίες εξ αποστάσεως μεταξύ πολλών παιχτών, χωρίς να απαιτείται αξιόπιστο τρίτο μέρος. Σημειώνουμε ότι παραδοσιακά, η κρυπτογραφία αφορούσε την απόκρυψη περιεχομένου, ενώ αυτός ο νέος τύπος υπολογισμού και πρωτοκόλλου αφορά την απόκρυψη μερικών πληροφοριών σχετικά με τα δεδομένα κατά τον υπολογισμό, με τα δεδομένα να προέρχονται από πολλές πηγές και τη σωστή εξαγωγή του αποτελέσματος. Σε αντίθεση με τα παραδοσιακά κρυπτογραφικά συστήματα, όπου η κρυπτογραφία διασφαλίζει την ασφάλεια και την ακεραιότητα της επικοινωνίας ή της αποθήκευσης και ο εισβολέας βρίσκεται εκτός του συστήματος των συμμετεχόντων, η κρυπτογραφία σε αυτό το μοντέλο προστατεύει το απόρρητο των συμμετεχόντων μεταξύ τους.

Τα ασφαλή MPC πρωτόκολλα, μελετούν μηχανισμούς που επιτρέπουν μια ομάδα N ανεξάρτητων συμμετεχόντων (p1 ,p2, p3… pN), ο καθένας από τους οποίους έχει ιδιωτικά δεδομένα (d1, d2, ..., dN), να υπολογίσουν συλλογικά μια συνάρτηση F(d1, d2, ..., dN). Κάθε συμμετέχων κρατά μυστική μια είσοδο (input), η οποία παραμένει κρυμμένη στα υπόλοιπα μέρη, αλλά χρησιμοποιείται για τον υπολογισμό της συνάρτησης. Οι συμμετέχοντες μαθαίνουν μόνο το τελικό αποτέλεσμα. Οποιαδήποτε συνάρτηση f που μπορεί να επιλυθεί σε πολυωνυμικό χρόνο μπορεί να αναπαρασταθεί ως πρωτόκολλο MPC. Η αξία των πρωτοκόλλων αυτών έγκειται στο ότι, για τον υπολογισμό της συνάρτησης F, δεν απαιτείται κάποια έμπιστη τρίτη οντότητα.

Για παράδειγμα, ας υποθέσουμε ότι έχουμε τρία μέρη Alice, Bob και Charlie, με αντίστοιχα στοιχεία x, y και z που υποδηλώνουν τους μισθούς τους. Θέλουν να μάθουν τον υψηλότερο από τους τρεις μισθούς, χωρίς να αποκαλύπτουν ο ένας στον άλλο το μέγεθός τους. Μαθηματικά, αυτό μεταφράζεται σε: F(x, y, z) = max(x, y, z). Αν υπήρχε κάποιος αξιόπιστος εξωτερικός συνεργάτης (ας πούμε, ότι είχαν έναν αμοιβαίο φίλο Tony που τον εμπιστεύονταν και γνώριζαν ότι θα μπορούσε να κρατήσει ένα μυστικό), θα μπορούσε ο καθένας να πει τον μισθό του στον Tony, ώστε να υπολογίσει το μέγιστο μισθό και να το πει σε όλους. Ο στόχος του MPC είναι να σχεδιάσει ένα πρωτόκολλο, όπου, ανταλλάσσοντας μηνύματα μόνο μεταξύ τους, η Alice, ο Bob και ο Charlie να μπορούν να μάθουν το αποτέλεσμα της F (x, y, z) χωρίς να αποκαλύψουν ποιος κάνει τι και χωρίς να χρειάζονται να βασιστούν στον Tony. Δεν πρέπει να μάθουν περισσότερα με την εμπλοκή τους στο πρωτόκολλό από ότι θα μάθαιναν αλληλεπιδρώντας με έναν άφθαρτο, απόλυτα αξιόπιστο Tony.

Με απλά λόγια, οι πιο βασικές ιδιότητες που στοχεύει να διασφαλίσει ένα πρωτόκολλο υπολογισμού πολλών μερών είναι:

- Απόρρητο εισόδου: Δεν μπορούν να συναχθούν πληροφορίες σχετικά με τα ιδιωτικά δεδομένα που κατέχουν τα μέρη από τα μηνύματα που αποστέλλονται κατά την εκτέλεση του πρωτοκόλλου. Οι μόνες πληροφορίες που μπορούν να συναχθούν σχετικά με τα ιδιωτικά δεδομένα είναι οτιδήποτε θα μπορούσε να συναχθεί από το να δούμε την έξοδο της συνάρτησης και μόνο.

- Ορθότητα: Οποιοδήποτε υποσύνολο των συμβαλλόμενων μερών που επιθυμούν, κατά παρέκκλιση της σωστής διαδικασίας, να μοιραστούν πληροφορίες ή να αποκλίνουν από τις οδηγίες κατά την εκτέλεση του πρωτοκόλλου, δεν θα πρέπει να είναι σε θέση να αναγκάσει τα έντιμα μέρη να παράγουν ένα λανθασμένο αποτέλεσμα. Αυτός ο στόχος ορθότητας έρχεται σε δύο φάσεις: είτε τα ειλικρινά μέρη εγγυώνται να υπολογίσουν τη σωστή έξοδο (ένα «ισχυρό» πρωτόκολλο), είτε ματαιώνουν εάν εντοπίσουν κάποιο σφάλμα (ένα πρωτόκολλο MPC «με ματαίωση»).

Ένα πρωτόκολλο υπολογισμού πολλαπλών μερών πρέπει να είναι ασφαλές για να είναι αποτελεσματικό. Στη σύγχρονη κρυπτογραφία, η ασφάλεια ενός πρωτοκόλλου σχετίζεται με μια απόδειξη ασφαλείας. Η απόδειξη ασφαλείας είναι μια μαθηματική απόδειξη όπου η ασφάλεια ενός πρωτοκόλλου ανάγεται σε εκείνη της ασφάλειας των συμμετεχόντων του. Ωστόσο, δεν είναι πάντα δυνατό να επαληθευτεί η ασφάλεια του κρυπτογραφικού πρωτοκόλλου με βάση τις γνώσεις του συμβαλλόμενου μέρους και την ορθότητα του πρωτοκόλλου. Για τα πρωτόκολλα MPC, το περιβάλλον στο οποίο λειτουργεί το πρωτόκολλο σχετίζεται με το πραγματικό παράδειγμα στον ιδανικό κόσμο. Τα συμβαλλόμενα μέρη δεν μπορούν να ισχυρίζονται ότι δεν γνωρίζουν τίποτα, αφού πρέπει να μάθουν την έξοδο του αποτελέσματος και η έξοδος εξαρτάται από τις εισόδους. Επιπλέον, η ορθότητα της παραγωγής δεν είναι εγγυημένη, δεδομένου ότι η ορθότητα του αποτελέσματος εξαρτάται από τις εισόδους των συμβαλλόμενων μερών και οι είσοδοι πρέπει να υποτεθούν ότι είναι διεφθαρμένοι.

Το Real World / Ideal World Paradigm δηλώνει δύο κόσμους: (i) Στο μοντέλο του ιδανικού κόσμου (ideal world), υπάρχει ένα άφθαρτο αξιόπιστο συμβαλλόμενο μέρος στο οποίο, κάθε συμμετέχων στο πρωτόκολλο, στέλνει τα στοιχεία του. Αυτό το αξιόπιστο μέρος υπολογίζει τη λειτουργία από μόνο του και στέλνει την κατάλληλη έξοδο σε κάθε μέρος. (ii) Αντίθετα, στο μοντέλο του πραγματικού κόσμου (real world), δεν υπάρχει αξιόπιστο μέρος και το μόνο πράγμα που μπορούν να κάνουν όλα τα μέρη, είναι να ανταλλάσσουν μηνύματα μεταξύ τους. Ένα πρωτόκολλο λέγεται ότι είναι ασφαλές εάν κάποιος δεν μπορεί να μάθει περισσότερα για τις ιδιωτικές εισροές κάθε μέρους στον πραγματικό κόσμο από ό, τι θα μπορούσε να μάθει στον

ιδανικό κόσμο. Στον ιδανικό κόσμο, δεν ανταλλάσσονται μηνύματα μεταξύ των μερών, επομένως τα μηνύματα που ανταλλάσσονται στον πραγματικό κόσμο δεν μπορούν να αποκαλύψουν μυστικές πληροφορίες. Πώς όμως ένα τέτοιο σύστημα μπορεί να χρησιμοποιηθεί σε εφαρμογές ιχνηλάτησης επαφών;

3.8.1 Ανίχνευση επαφών με ασφαλή υπολογισμό πολλαπλών μερών

Έστω λοιπόν ότι έχουμε ένα σύστημα όπως περιγράφεται στο [1], το οποίο βασίζεται στην αξιοποίηση της Υγειονομικής Αρχής (Health Authority-HA) και η οποία συλλέγει το ιστορικό των τοποθεσιών των χρηστών που έχουν νοσήσει, όπως έχει γίνει σε πολλές χώρες που έχουν πληγεί από την πανδημία. Υποθέτουμε ακόμα, ότι η συντριπτική πλειονότητα των ατόμων, χρησιμοποιούν υπηρεσίες βάσει τοποθεσίας που τις αποθηκεύουν τοπικά. Για την ανάλυση απειλών του μοντέλου αυτού, οι συμμετέχοντες θεωρούνται μερικώς ειλικρινείς (semi-honest). Η Υγειονομική Αρχή μπορεί να χρησιμοποιήσει τα σημεία δεδομένων των μολυσμένων ασθενών (και τις σχετικές χρονικές σημάνσεις) για να αρχικοποιηθεί το MPC με όλους όσους θέλουν να ανιχνεύσουν τους εαυτούς τους. Κατά τη διάρκεια αυτής της αξιολόγησης, κάθε άτομο πρέπει να εγκαθιδρύσει επικοινωνία με την υγειονομική Αρχή. Μαζί, τα συμβαλλόμενα μέρη καθορίζουν πού διασταυρώνονται οι περιοχές των μολυσμένων και των μη μολυσμένων ατόμων. Η ανίχνευση επαφών γίνεται ιδιωτικά, ώστε μόνο το άτομο που νόσησε να γνωρίζει την κατάστασή του. Καμία πληροφορία για παλιές τοποθεσίες των ατόμων που έχουν νοσήσει δεν αποκαλύπτεται στα συμβαλλόμενα μέρη.

Ο αλγόριθμος ανίχνευσης επαφών MPC επιτρέπει στις εισόδους και στις εξόδους να παραμένουν κρυμμένες από τα υπόλοιπα μέρη. Οι τοποθεσίες εισόδου l: = (x; y; t) αποτελούνται από γεωγραφικές συντεταγμένες(x,y) και ένα χρονικό στοιχείο(t). Το υψόμετρο της τοποθεσίας αγνοείται, καθώς είναι επιρρεπής σε σφάλματα. Κάθε χρήστης ‘u’ έχει ‘m’ τοποθεσίες που πρέπει να ελεγχθούν στο ιστορικό τοποθεσίας τους. Η Υγειονομική Αρχή διατηρεί έναν αριθμό ‘n’ από δεδομένα τοποθεσίας ‘l’ των μολυσμένων ατόμων. Έπειτα υπολογίζεται ένα σύνολο από ‘L’ τοποθεσίες για τις οποίες η Ευκλείδεια απόσταση σε σχέση με το ‘l’ είναι μικρότερη από μία ορισμένη τιμή που έχει δοθεί από το πρωτόκολλο (κατώφλι). Η Υγειονομική Αρχή και ο χρήστης, υπολογίζουν το ‘L’για όλα τα αντίστοιχα σημεία δεδομένων. Μόνο ο χρήστης μαθαίνει το τελικό αποτέλεσμα. Το πρωτόκολλο εγγυάται ότι καμία πληροφορία δεν αποκαλύπτεται στα υπόλοιπα συμβαλλόμενα μέρη ή στην Υγειονομική Αρχή.

Ως μειονεκτήματα αυτού του πρωτοκόλλου είναι αρχικά μια Υγειονομική Αρχή που δεν δρα όπως πρέπει ως έμπιστη οντότητα, θα μπορούσε να προκαλέσει πανικό με το να αυξήσει τις τοποθεσίες που έχουν πληγεί από την πανδημία αλλά και η χρήση του πρωτοκόλλου σε κεντρικοποιημένες υλοποιήσεις, αυξάνει σημαντικά τους χρόνους υπολογισμών του συστήματος.

Επιπλέον [11], κακόβουλοι χρήστες ενδέχεται να το εκμεταλλευτούν για να το κάνουν (D) DoS επιθέσεις, εκτός εάν έχουν αναπτυχθεί κατάλληλα αντίμετρα. Ένα άλλο ζήτημα είναι την έλλειψη λεπτομερειών σχετικά με τον υπολογισμό των κινδύνων μόλυνσης, οι οποίοι βασίζονται στην εγγύτητα και των δύο γραμματοσήμων και των συντεταγμένων γεωγραφικής θέσης. Δεν είναι σαφές πώς για να οριστεί ένα κατώφλι στις χρονικές σφραγίδες, λαμβάνοντας υπόψη ότι υπάρχει μια ποικιλία μοτίβων κινητικότητας μεταξύ των ενδιαφερόμενων χρηστών.

Κεφάλαιο 4

Επιθέσεις και Ευπάθειες των Συστημάτων Ιχνηλάτησης

Τα συστήματα ιχνηλάτησης επαφών θα πρέπει να είναι έγκυρα όσον αφορά τα θετικά και τα αρνητικά αποτελέσματα των κρουσμάτων. Αυτό σημαίνει ότι αρχικά δεν θα πρέπει να αποθηκεύουν αναγνωριστικά εγγύτητας τα οποία έχουν χρονική διάρκεια μικρότερη από 15 λεπτά γιατί αυτό θα οδηγήσει σε λανθασμένα αποτελέσματα. Εάν δηλαδή κάποιος περιμένει στη στάση του λεωφορείου μαζί με άλλον χρήστη, τα αναγνωριστικά που ανταλλάσσονται μεταξύ τους δεν θα πρέπει να λαμβάνονται υπόψη. Όπως επίσης δεν θα πρέπει να λαμβάνονται υπόψη τα αναγνωριστικά που μεταδίδονται μεταξύ ατόμων που μένουν σε διπλανά σπίτια γιατί πρακτικά δεν έχουν έρθει σε επαφή. Το στάδιο αυτό της εφαρμογής είναι εξαιρετικά σημαντικό διότι τα λανθασμένα αποτελέσματα θα έχουν ως αποτέλεσμα να χάσουν οι χρήστες την

εμπιστοσύνη τους στο σύστημα, να τους αποτρέψει από το να χρησιμοποιούν την εφαρμογή ιχνηλάτησης και εν τέλει να οδηγήσει στην κατάρρευση του συστήματος.

Όταν αξιολογούμε ένα σύστημα ιχνηλάτησης, είναι σημαντικό να αναφέρουμε τους τύπους των εισβολέων από τους οποίους κινδυνεύει. Αρχικά έχουμε τους ημι- ειλικρινείς (semi-honest), οι οποίοι πολλές φορές αποκαλούνται ως «ειλικρινείς αλλά περίεργοι» (honest but curious) οι οποίοι ακολουθούν μεν το πρωτόκολλο, αλλά ενδιαφέρονται να μάθουν όσο περισσότερη πληροφορία γίνεται και τους κακοήθεις οι οποίοι θέλουν να προκαλέσουν ζημία σε ένα τέτοιο σύστημα.

Αρχικά ας δούμε κάποιους ορισμούς που θα χρησιμοποιηθούν στη συνέχεια

- Αυτόματο Σύστημα Ιχνηλάτησης (automated contact tracing system-ACT)
- Υγειονομική Αρχή (health authority- HA) της κάθε χώρας
- Χρήστες (Users), οι οποίοι θέλουν να δουν την κατάσταση υγείας τους μέσω του συστήματος ιχνηλάτησης
- Άτομα που νόσησαν, οι οποίοι έχουν νοσήσει από τον ιό και «ανεβάζουν» την κατάσταση τους στον διακομιστή
- Φορέας παροχής υπηρεσιών
- Φορέας παροχής δικτύου

4.1 Επιθέσεις στα κεντρικοποιημένα συστήματα

Επιθέσεις μπορεί να γίνουν από άτομα με διάφορα κίνητρα, όπως από άτομα που αμφισβητούν τον ιό και την ύπαρξή του αλλά και άτομα που θέλουν απλά να προκαλέσουν κακό λόγω διαφόρων σκοπιμοτήτων. Αφού τα κεντρικοποιημένα συστήματα, στηρίζονται σε έναν κεντρικό διακομιστή πρέπει να δοθεί έμφαση στην προστασία του από κακόβουλες επιθέσεις.

4.1.1 Replay/Relay επιθέσεις

Μια τέτοια επίθεση[13] μπορεί να οδηγήσει στο να ανακηρυχθούν υγιή άτομα ως «κρούσματα». Το μόνο που χρειάζεται ένας εισβολέας είναι να διαθέτει κεραίες ώστε να μπορέσει να προωθήσει αναγνωριστικά από έμπιστους χρήστες στην ίδια ή και διαφορετική περιοχή. Για να αποκαλείται Replay/Relay η επίθεση θα πρέπει τα αναγνωριστικά αυτά να είναι γνήσια (αλλιώς αναφερόμαστε σε επίθεση άρνησης της υπηρεσίας «Denial Of Service-DoS attack»). Όταν λάβει μέρος η επίθεση, οι χρήστες λαμβάνουν από τον διακομιστή το μήνυμα ότι βρίσκονται σε κίνδυνο μιας και έχουν έλθει σε επαφή με νοσούν άτομο και τους προτρέπει να μείνουν σε καραντίνα ή να πάνε να εξεταστούν. Αυτή η επίθεση γίνεται ακόμα πιο σοβαρή όταν ο εισβολέας προωθεί αναγνωριστικά από νοσοκομεία και περιοχές γεμάτα με θετικά κρούσματα. Καθώς σε ένα κεντρικοποιημένο σύστημα το TempID (όπως έχει προαναφερθεί) έχει ένα χρονικό όριο λήξης (περίπου 15 λεπτών), η Replay επίθεση μπορεί να λάβει μέρος πριν τη λήξη του.

4.1.2 Επιθέσεις εξάντλησης ενέργειας και χώρου

Η επίθεση εξάντλησης ενέργειας και χώρου [13] είναι μια επίθεση άρνησης της υπηρεσίας η οποία περιλαμβάνει μεγάλο όγκο μηνυμάτων. Όταν ένας εισβολέας στείλει σε μία κοντινή συσκευή μεγάλο όγκο μηνυμάτων, η συσκευή μέσω της εφαρμογής θα ελέγξει εάν τα μηνύματα αυτά είναι γνήσια ή όχι. Αν δεν είναι γνήσια, τα απορρίπτει με κόστος την εξάντληση της ενέργειας (εδώ ουσιαστικά αναφερόμαστε στην μπαταρία της). Αν είναι γνήσια, τότε η εφαρμογή αναγκάζεται να αποθηκεύσει τα αναγνωριστικά που συνοδεύουν τα μηνύματα, με αποτέλεσμα να γεμίζει ο χώρος της συσκευής και να είναι συνεχώς απασχολημένη στο να διαχειρίζεται μηνύματα και αναγνωριστικά τα οποία τελικά, είναι άχρηστα για το χρήστη και να μη της μένει χρόνος και ενέργεια να διαχειριστεί μηνύματα από γνήσιους χρήστες. Αυτή η επίθεση γίνεται περισσότερο επικίνδυνη όταν ο χρήστης βρίσκεται σε ένα πολυσύχναστο μέρος όπου κάθε μήνυμα του εισβολέα απευθύνεται σε πολλά άτομα. Μπορεί μια τέτοια επίθεση να μη φαίνεται σοβαρή, όμως ας αναλογιστούμε τι θα συμβεί εάν ο χρήστης παρατηρήσει ότι η κινητή του συσκευή γίνεται αργή και δεν μπορεί να εκτελέσει άλλες εφαρμογές ή ότι του τελειώνει πολύ γρήγορα η μπαταρία. Τότε το πιο πιθανό είναι να θελήσει να διαγράψει την εφαρμογή από τη συσκευή του και το ίδιο να κάνουν και οι υπόλοιποι χρήστες. Ένα τέτοιο γεγονός θα αποβεί μοιραίο στο σύστημα ιχνηλάτησης και στην εν γένει κατάρρευσή του. Το[13] προτείνει να υπάρχει ένας μηχανισμός στην εφαρμογή ο οποίος ελέγχοντας τα μηνύματα του εισβολέα να τα

απορρίπτει και να ειδοποιεί το χρήστη να εγκαταλείψει την περιοχή και να ενημερώσει το διακομιστή για το συμβάν της επίθεσης.

4.1.3 Trolling επιθέσεις

Η επίθεση αυτή γίνεται από κάποιον ο οποίος έχει βρεθεί θετικός με στόχο να εξαπατήσει και άλλα άτομα είτε επειδή θέλει να σπείρει πανικό σε συγκεκριμένα άτομα είτε επειδή νιώθει θυμωμένος και απογοητευμένος με τον εαυτό του και με τους άλλους. Μια τέτοια επίθεση θα μπορούσε να πραγματοποιηθεί εάν ο εισβολέας, αφού πρώτα έχει ενημερώσει το διακομιστή ότι έχει νοσήσει από τον ιό, τοποθετήσει τη συσκευή του σε ένα ταξί, σε ένα σκύλο ή σε ένα drone και καθώς κυκλοφορεί ελεύθερα έξω, η συσκευή στέλνει αναγνωριστικά σε κοντινές συσκευές με αποτέλεσμα ο διακομιστής να ενημερώσει τους χρήστες ότι υπάρχει ο κίνδυνος να έχουν έρθει σε επαφή με άτομο που νοσεί και να μείνουν σε καραντίνα ή να προβούν σε διαγνωστικό τεστ. Ένα τέτοιο γεγονός θα οδηγήσει σε σπατάλη των υγειονομικών πόρων, σε πανικό των ατόμων και στο να πάψουν να έχουν εμπιστοσύνη στο σύστημα και στα διαγνωστικά τεστ. Για να αποφευχθεί η επίθεση, το[13] προτείνει σε μία τέτοια μαζική εισροή των ατόμων για τεστ, οι Υγειονομικές Αρχές να ελέγξουν αν είναι απόρροια ίδιου διαγνωστικού αναγνωριστικού το οποίο ποικίλει από τόπο σε τόπο ώστε να αναλάβουν δράση.

4.1.4 Επιθέσεις συσχετισμού

Οι επιθέσεις συσχετισμού (linking attacks)[13], αποσκοπούν στην παραβίαση της ιδιωτικότητας ανακαλύπτοντας μηνύματα ως συνδεδεμένα (δηλαδή ότι αντιστοιχούν στον ίδιο χρήστη), παρόλο που προορίζονταν να εμφανιστούν ως «αποσυνδεδεμένα». Έστω δηλαδή ότι ο εισβολέας θέλει να συσχετίσει δύο μηνύματα ότι προέρχονται από τον ίδιο αποστολέα, παρόλο που μία τέτοια συσχέτιση δεν θα έπρεπε να είναι εφικτή. Ο εισβολέας χρησιμοποιεί μια συσκευή λήπτη με κανονική συχνότητα ανταλλαγής μηνυμάτων και κανονική ισχύ σήματος Bluetooth και βρίσκεται σε σταθερή τοποθεσία για διάρκεια ικανή να λάβει μηνύματα από οποιαδήποτε κοντινή συσκευή. Δύο μηνύματα είναι πιθανό να συνδεθούν όταν η διαφορά λήψης τους είναι αντίστοιχη με την κανονική συχνότητα ανταλλαγής μηνυμάτων. Ως αποτέλεσμα έχουμε να μειώνεται το απόρρητο κοντινών ατόμων. Το πρόβλημα μεγαλώνει εάν η επίθεση λάβει χώρο σε πολυσύχναστο μέρος και οδηγήσει έτσι τον κόσμο στο να απ ’εγκαταστήσει την εφαρμογή. Για να μετριαστεί η επίθεση, θα πρέπει να η κινητή συσκευή να μεταβάλλει την ισχύ σήματος ώστε να δυσκολέψει τον εισβολέα να πάρει τα μηνύματα από κοντινά πρόσωπα. Να τον «αναγκάσει»

δηλαδή, να πρέπει δηλαδή να ακολουθεί το κοντινό άτομο για πολλή ώρα ώστε να καταφέρει να πραγματοποιήσει την επίθεση.

4.1.5 Επίθεση άρσης ψευδωνυμοποίησης και παρακολούθησης

Ο κίνδυνος της άρσης ψευδωνυμοποίησης των εφήμερων αναγνωριστικών [13]θα μπορούσε να βοηθήσει τους εισβολείς να εντοπίσουν/αναγνωρίσουν τους χρήστες. Το κύριο πρόβλημα των κεντρικοποιημένων συστημάτων είναι ότι επιτρέπουν αυτές τις επιθέσεις σε μεγάλο βαθμό, εάν η ασφάλεια του κεντρικού διακομιστή έχει διαρραγεί, ή εάν η αρχή είναι διεφθαρμένη. Εάν κάποιος εισβολέας αποκτήσει πρόσβαση στο κανάλι με το οποίο «επικοινωνούν» διακομιστής και εφαρμογή θα μπορεί αποκαλύψει τα ψευδώνυμα που ανταλλάσσονται μεταξύ τους και έτσι να αντιστοιχίσει τα ψευδώνυμα με τις ταυτότητες των χρηστών. Αυτό θα μπορούσε να αποφευχθεί εάν υπάρχει μια εξουσιοδοτημένη αρχή η οποία παρακολουθεί τον διακομιστή και ελέγχει τα κανάλια επικοινωνίας του και να μετριαστεί εάν το μυστικό κλειδί δημιουργείται περιοδικά.

4.1.6 Επίθεση άρνησης της υπηρεσίας

Ο στόχος αυτής της επίθεσης είναι να καταναλώσει τους πόρους (μπαταρία, εύρος ζώνης, επεξεργασία κ.λπ.) τα οποία είναι διαθέσιμα στο σύστημα (χρήστης κινητό, διακομιστής)[13]. Σε αυτό το πλαίσιο, συζητάμε την επίθεση ψευδών μηνυμάτων/σημάτων στο περιβάλλον παρακολούθησης επαφών. Αυτό γίνεται καταναλώνοντας την μπαταρία κινητών συσκευών, προκαλώντας μεταφόρτωση των ψευδών μηνυμάτων στον διακομιστή όταν ένας χρήστης διαγνωστεί θετικός και αυξάνοντας τον χρόνο επεξεργασίας στο διακομιστή και στην κινητή συσκευή. Σημειώνουμε ότι στην κεντρικοποιημένη υλοποίηση, ο διακομιστής θα επεξεργαστεί τα ψεύτικα μηνύματα εγγύτητας, αλλά θα τα απορρίψει μετά τον έλεγχο εγκυρότητας.

4.2 Επιθέσεις στα αποκεντρωμένα συστήματα

Οι επιθέσεις και σε αυτά τα συστήματα μπορεί να λάβουν μέρος από άτομα με διάφορα κίνητρα, πολιτικά, θρησκευτικά ή ιδεολογικά. Αφού τα αποκεντρωμένα συστήματα στηρίζονται κυρίως στις κινητές συσκευές και όχι τόσο στον διακομιστή, θα πρέπει να δοθεί έμφαση στην προστασία τους ώστε να αποφευχθούν οι επιθέσεις που αναλύουμε παρακάτω.

4.2.1 Replay/Relay επιθέσεις

Η Replay/Relay επίθεση[13] όπως και προηγουμένως, μπορεί να οδηγήσει σε λανθασμένη διάγνωση υγιών ατόμων. Αυτό συμβαίνει όταν ένας εισβολέας προωθεί μηνύματα από έγκυρους χρήστες στην ίδια ή και διαφορετική διεύθυνση. Τα αναγνωριστικά στα αποκεντρωμένα συστήματα είναι έγκυρα στο διάστημα της μιας ώρας ενώ η τρέχουσα χρονική σήμανση είναι με ακρίβεια ενός λεπτού. Η εφαρμογή πιστοποιεί τη χρονική στιγμή που παρέλαβε τα αναγνωριστικά και τη συγκρίνει με τη χρονική στιγμή που αυτά δημιουργήθηκαν και ελέγχει αν ταιριάζουν. Αυτός ο μηχανισμός εξασφαλίζει την ασφάλεια του συστήματος σε Replay επιθέσεις, ενώ δεν την εξασφαλίζει σε Relay επιθέσεις διότι τα αναγνωριστικά παραμένουν έγκυρα.

4.2.2 Επίθεση Paparazzi

Ένας paparazzi μπορεί να πάρει το εφήμερο αναγνωριστικό ενός ατόμου και μετά να αναγνωρίσει το άτομο αυτό, εάν αποδειχθεί θετικά διαγνωσμένος. Μια λύση που προτείνεται από το DP3T πρωτόκολλο[4] είναι να μεταδίδονται τα αναγνωριστικά τμηματικά για να είναι δύσκολα για κάποιον να τα συλλέξει.

4.2.3 Nerd επίθεση

Οποιοδήποτε άτομο Α[4], μπορεί να χρησιμοποιήσει μια εφαρμογή που συλλέγει εφήμερα αναγνωριστικά και «ρωτάει» τον Α αν θέλει να απομνημονεύσει την ταυτότητα του Β μπροστά του. Στη συνέχεια, ελέγχει τακτικά στον διακομιστή για αναφερόμενες περιπτώσεις και ενημερώνει τον Α για αναγνωρισμένες περιπτώσεις.

4.2.4 Στρατιωτική επίθεση

Αυτός ο τύπος επίθεσης είναι μια γενίκευση της επίθεσης nerd[4] στην οποία μια ομάδα ανθρώπων συγκεντρώνει τα εφήμερα αναγνωριστικά για να αναγνωρίσει όσους χρήστες ανέφεραν ότι είναι θετικά διαγνωσμένοι.

4.2.5 Επίθεση Οργανισμού (Organization Attack)

Ένας οργανισμός όπως το ξενοδοχείο[4], ένα κατάστημα ή μια εταιρεία, μπορεί να εγκαταστήσει έναν συλλέκτη Bluetooth στο μέρος των επισκεπτών ώστε να μπορεί να συλλέξει τα εφήμερα αναγνωριστικά τους. Ο οργανισμός αναγνωρίζει το πρόσωπο των επισκεπτών του στην είσοδο και ως εκ τούτου, μπορεί να συλλέξει πολλές πληροφορίες και στη συνέχεια αυτές τις πληροφορίες να τις πουλήσει ή να τις καταχραστεί, εάν τα άτομα που αφορούν διαγνωστούν θετικά στον ιό.

4.2.6 Επίθεση από κακόβουλο λογισμικό

Ο εισβολέας μπορεί να είναι ένα κακόβουλο λογισμικό –δηλαδή εφαρμογή που θα είναι εγκατεστημένη στη κινητή συσκευή του χρήστη και θα συλλέγει τα εφήμερα αναγνωριστικά μιας γνήσιας εφαρμογής ιχνηλάτησης τόσο αυτά που μεταδίδονται όσο και αυτά που συλλέγονται[4]. Οι εφαρμογές αυτές θα μπορούσαν να έχουν πρόσβαση και σε προσωπικά δεδομένα που αποθηκεύονται στην κινητή συσκευή του χρήστη όπως στο ημερολόγιο, το GPS, το μικρόφωνο αλλά και την κάμερα και να εντοπίσουν οποιαδήποτε επαφή έχει διαγνωστεί θετικά. Μια λύση για αυτήν την επίθεση την προτείνει το GAEN [5]το οποίο δεν αφήνει ποτέ καμία εφαρμογή που εκτελείται στο παρασκήνιο να έχει πρόσβαση στο BLE.

4.2.7 Επίθεση από κακόβουλο λειτουργικό σύστημα ή υλικό

Στην επίθεση αυτή το λειτουργικό σύστημα θα μπορούσε να συλλέξει τα εφήμερα αναγνωριστικά μιας γνήσιας εφαρμογής ιχνηλάτησης. Δεδομένου ότι η εφαρμογή δίνει το εφήμερο αναγνωριστικό στο λειτουργικό σύστημα που το δίνει το υλικό, δεν είναι δυνατή η προστασία από αυτήν την περίπτωση κακόβουλων λειτουργικών συστημάτων.

4.2.8 Επίθεση συνδυασμένη με παρακολούθηση βίντεο

Μια κακόβουλη τοπική αρχή[4] εγκαθιστά ένα σύστημα παρακολούθησης βίντεο με αισθητήρα Bluetooth και θα μπορούσε να αποθηκεύσει σε μια βάση δεδομένων ζεύγη που αποτελούνται από το καταγεγραμμένο εφήμερο αναγνωριστικό και έναν δείκτη του εγγεγραμμένου βίντεο. Αργότερα, τα συλλεγόμενα αναγνωριστικά μπορούν να αντιστοιχιστούν σε αναφερόμενες περιπτώσεις με άμεσο σημείο αναφοράς το βίντεο.

4.2.9 Επίθεση παρακολούθησης και άρσης ψευδωνυμοποίησης

Οι επιθέσεις παρακολούθησης και άρσης της ψευδωνυμοποίησης[4] στόχο έχουν να πλήξουν την ιδιωτικότητα των χρηστών. Ο εισβολέας στόχο έχει να αποκαλύψει την ταυτότητα του χρήστη που νοσεί. Για παράδειγμα θα μπορεί ο εισβολέας να παρακολουθεί το σήμα του Bluetooth των χρηστών καθώς επίσης και την τοποθεσία τους και να χρησιμοποιεί αυτές τις πληροφορίες για να αποκαλύψει την ταυτότητά τους όταν κάποιος από αυτούς ανακηρυχθεί ως θετικός. Εάν αυτή η επίθεση λάβει μέρος σε πολυσύχναστο μέρος, τότε η ταυτότητα πολλών χρηστών θα αποκαλυφθεί και θα οδηγήσει το σύστημα σε κατάρρευση μιας και θα χάσουν την εμπιστοσύνη τους σε αυτό.

4.3 Κοινές Ευπάθειες των δύο συστημάτων

Υπάρχουν ευπάθειες και ελαττώματα τα οποία εμφανίζονται και στα δύο προαναφερθέντα συστήματα.

4.3.1 Αποφυγή λανθασμένων θετικών αναφορών κρουσμάτων

Τα συστήματα ιχνηλάτησης[4], (τόσο τα κεντρικοποιημένα όσο και τα αποκεντρωμένα), θα πρέπει να διασφαλίσουν ότι μόνο οι θετικά διαγνωσμένοι χρήστες από επίσημο υγειονομικό φορέα μπορούν να ανακηρυχθούν ως «θετικοί» και ως εκ τούτου να μπορούν να «ανεβάσουν» στο διακομιστή τις επαφές τους. Εάν ο οποιοσδήποτε χρήστης ανακοίνωνε στο διακομιστή ότι έχει μολυνθεί από τον ιό, τότε το σύστημα θα κατέληγε σε λανθασμένα αποτελέσματα και θα οδηγούμασταν στην κατάρρευσή του. Θα πρέπει οι υγειονομικές αρχές για τα διαγνωστικά τεστ που κάνουν να στέλνουν έναν κωδικό πιστοποίησης ή ένα barcode και μόνο αν αυτό είναι γνήσιο να μπορούν να δηλώσουν ότι είναι θετικά διαγνωσμένοι και να ανεβάσουν τις επαφές τους στον διακομιστή.

4.3.2 Διαλειτουργικότητα των εφαρμογών ιχνηλάτησης

Οι εφαρμογές ιχνηλάτησης θα πρέπει να λειτουργούν σωστά και μεταξύ τους, όταν ένας χρήστης ταξιδεύει από μία χώρα στην άλλη, αλλά και όταν βρίσκονται κοντά στα σύνορα.

4.3.3 Συμβατότητα των εφαρμογών ιχνηλάτησης

Οι εφαρμογές θα πρέπει να είναι συμβατές με όλα τις έξυπνες συσκευές ανεξάρτητα από την έκδοση του λογισμικού που χρησιμοποιούν γιατί αυτό αποτρέπει τον κόσμο από το να τη χρησιμοποιήσει μιας και δεν έχουν όλοι την οικονομική δυνατότητα να αγοράσουν τελευταίας τεχνολογίας κινητές συσκευές. Ένα παράδειγμα είναι η εφαρμογή της Αγγλίας η nhs Covid-19 η οποία δεν λειτουργεί σε έκδοση android 5.

4.3.4 Εξαναγκασμός και κλοπή

Και τα δύο συστήματα δεν μπορούν να ανταπεξέλθουν εάν κάποιος κλέψει την κινητή συσκευή του χρήστη ή εάν τον εξαναγκάσει ένας εισβολέας ή ένας οργανισμός να αποκαλύψει τα στοιχεία της κινητής συσκευής του.

4.3.5 Αποκάλυψη του κοινωνικού γραφήματος

Καταρχάς πρέπει να αναφέρουμε ότι καμία αποκάλυψη δεν γίνεται από τη στιγμή που καμία επαφή του χρήστη δεν αναφερθεί ως θετικά διαγνωσμένη στον ιό. Τα κεντρικοποιημένα συστήματα αποκαλύπτουν τον κοινωνικό γράφο (social graph) στον διακομιστή και μόνο, αν υποθέσουμε ότι ο διακομιστής είναι ασφαλής και δρα νόμιμα. Αλλά επειδή και τα αποκεντρωμένα συστήματα έχουν διακομιστή αυτός ο κίνδυνος παραμένει και σε αυτά τα συστήματα. Βέβαια και στα δύο αν κάποιος χρήστης ειδοποιηθεί ότι έχει έρθει σε επαφή με κάποιον που διαγνώστηκε θετικός, τότε μπορεί να καταλάβει με ποιους έχει έρθει σε επαφή και να ανακαλύψει την ταυτότητά τους.

4.3.6 Το δικαίωμα της επιλογής

Οι χρήστες των εφαρμογών έχουν τη δυνατότητα να μην εγκαταστήσουν την εφαρμογή, να απενεργοποιήσουν το Bluetooth τους και να αρνηθούν να αναφέρουν στις Υγειονομικές Αρχές ότι έχουν διαγνωστεί ως θετικοί. Όλα τα παραπάνω οδηγούν στη μη αποτελεσματικότητα της εφαρμογής ως προς την υποβοήθηση ιχνηλάτησης επαφών (βέβαια, όπως θα δούμε στη συνέχεια, το δικαίωμα της επιλογής στη συγκεκριμένη περίπτωση είναι στενά συνυφασμένο με το δικαίωμα της ελευθερίας αποφάσεων του ατόμου για τα προσωπικά του δεδομένα).

4.3.7 Μπλοκάρισμα του BLE

Ένας οργανισμός ή μια εταιρεία (για να μη κλείσει) θέλοντας να σταματήσει το σύστημα ιχνηλάτησης επαφών θα μπορούσε να μπλοκάρει την ανταλλαγή των ψευδωνύμων με το να μπλοκάρει τα κανάλια επικοινωνίας τους. Το τονίζει μάλιστα ότι θα πρέπει όλα τα συστήματα που στηρίζονται στο BLE, να μην επιτρέπουν το «ταίριασμα» των BLE συσκευών διότι με αυτόν τον τρόπο θα μπορούσε ένας εισβολέας να παρατηρήσει ότι το BLE είναι «ανοιχτό» σε κάποιες συσκευές και να προσπαθήσει να αποκτήσει μη εξουσιοδοτημένη πρόσβαση στις συσκευές αυτές.

4.3.8 Αποκάλυψη IP διεύθυνσης

Τα συστήματα ιχνηλάτησης στηρίζονται στο να μη γίνεται αποκάλυψη της IP διεύθυνσης του χρήστη στις Υγειονομικές Αρχές, γεγονός όμως που μπορεί να γίνει, ανεξάρτητα με το σύστημα ιχνηλάτησης που χρησιμοποιούν οι χρήστες. Στο [2] προτείνουν ότι για να νιώθουν (αλλά και για να είναι εντέλει ασφαλείς οι χρήστες) θα μπορούσαν να χρησιμοποιούν έναν διακομιστή μεσολάβησης(proxy) όπως ο Tor ή συνδυασμό δικτύων ώστε να μην αποκαλύπτεται η διεύθυνση και συνεπώς η ταυτότητα του χρήστη.

Κεφάλαιο 5

Νομικό πλαίσιο προστασίας προσωπικών δεδομένων

Όπως αναφέρθηκε και προηγουμένως, οι κινητές συσκευές είναι πολύ ευάλωτες και λιγότερο προστατευμένες από ότι είναι ένας διακομιστής. Ο χρήστης μπορεί να χάσει τη συσκευή του, να του την κλέψουν και να αποκαλυφθούν πολύτιμες πληροφορίες για άλλους χρήστες και ιδιαίτερα για αυτούς που νοσούν. Ας δούμε όμως αρχικά τι εννοούμε όταν αναφερόμαστε σε «ευαίσθητα δεδομένα», τι ορίζει ο Γενικός Κανονισμός Προστασίας Δεδομένων (ΓΚΠΔ) και πως διαχειρίζεται το κάθε σύστημα που προαναφέραμε τα ευαίσθητα δεδομένα.

5.1 Η έννοια της ιδιωτικότητας

Η έννοια της ιδιωτικότητας (privacy) υπάρχει ως κοινωνικό ζήτημα εδώ και πολλούς αιώνες και αποτελεί μια από τις βασικές ανάγκες του ατόμου. Οι Αμερικανοί νομικοί Samuel Warren και Louis Brandeis με το άρθρο τους «Το δικαίωμα στην ιδιωτικότητα» το 1890, ορίζουν την ιδιωτικότητα ως το «Δικαίωμα να παραμένει κάποιος μόνος του». Ο F.Schoeman το 1984 την αναφέρει ως μια κατάσταση περιορισμένης πρόσβασης στο άτομο και τις πληροφορίες για την προσωπική του ζωή, ενώ ο πιο αποδεκτός ορισμός της έννοιας «ιδιωτικότητα» δόθηκε από τον νομικό Alan F.Westin ο οποίος αναφέρει την ιδιωτικότητα ως την ικανότητα του ατόμου να ελέγχει τους όρους υπό τους οποίους οι προσωπικές του πληροφορίες αποκτώνται και χρησιμοποιούνται από τους υπόλοιπους με τους οποίους επικοινωνούν.

Η προστασία της ιδιωτικής ζωής αναγνωρίζεται ως ένα θεμελιώδες ανθρώπινο δικαίωμα στην Ευρωπαϊκή Σύμβαση Δικαιωμάτων του Ανθρώπου (ΕΣΔΑ) το 1950 στο άρθρο 8 ως «Παν πρόσωπον δικαιούται εις τον σεβασμόν της ιδιωτικής και οικογενειακής ζωής του, της κατοικίας του και της αλληλογραφίας του», ενώ το 1981 το Συμβούλιο της Ευρώπης στη σύμβαση 108 για την Προστασία του Ατόμου από την Αυτοποιημένη Επεξεργασία Προσωπικών Δεδομένων αναφέρει ότι «Οι πληροφορίες προσωπικού χαρακτήρα που αποκαλύπτουν τη φυλετική προέλευση, τα πολιτικά φρονήματα, τις θρησκευτικές ή άλλες πεποιθήσεις, όπως και οι πληροφορίες προσωπικού χαρακτήρα που σχετίζονται με την υγεία ή την σεξουαλική ζωή, δεν δύνανται να αποτελέσουν αντικείμενο αυτοματοποιημένης επεξεργασίας, εάν το εσωτερικό δίκαιο δεν προβλέπει κατάλληλες εγγυήσεις. Το αυτό ισχύει για τις πληροφορίες προσωπικού χαρακτήρα που αφορούν ποινικές καταδίκες». Επομένως λοιπόν, η ιδιωτικότητα είναι στενά συνυφασμένη με την προστασία προσωπικών δεδομένων.

5.1.1 Ιδιωτικότητα και προσωπικά δεδομένα

Ως προσωπικά δεδομένα (ή δεδομένα προσωπικού χαρακτήρα) θεωρείται κάθε πληροφορία που αναφέρεται σε φυσικό πρόσωπο (ταυτοποιημένο ή ταυτοποιήσιμο). Για παράδειγμα, προσωπικά δεδομένα για ένα άτομο αποτελούν το όνομά του, η διεύθυνσή του, το τηλέφωνο του, τα ενδιαφέροντά του, οι απόψεις του, η εικόνα του σε φωτογραφίες και βίντεο κοκ.

Ο ορισμός των προσωπικών δεδομένων είναι εξαιρετικά ευρύς: αν μία πληροφορία που σχετίζεται με ένα άτομο υπάρχει η πιθανότητα αναγνώρισης/ ταυτοποίησής του, έστω και υπό

προϋποθέσεις που μπορούν να συντρέξουν, τότε η πληροφορία αυτή αποτελεί προσωπικό δεδομένο. Εξ αυτού, αναγνωριστικά συσκευών (πχ IMEI συσκευής, ANDROID ID) ή διευθύνσεων δικτύου συσκευής (IP διεύθυνσης κτλ) που χρησιμοποιεί ένας χρήστης, αποτελούν προσωπικά του δεδομένα.

Με την ανάπτυξη της τεχνολογίας και του διαδικτύου στη σημερινή εποχή, η συλλογή των πληροφοριών καθίσταται ιδιαίτερη εύκολη καθώς χιλιάδες δεδομένα μεταφέρονται και ανταλλάσσονται από διεθνή δίκτυα σε ελάχιστο χρόνο. Καθώς όμως τα συστήματα αυτά αναπτύσσονται και χρησιμοποιούνται από ολοένα και περισσότερους ανθρώπους, ελλοχεύουν κίνδυνοι όσον αφορά την προστασία της ιδιωτικότητας τους και των προσωπικών τους δεδομένων. Η ανάγκη λοιπόν προστασίας της ιδιωτικής ζωής των ανθρώπων, η ανάγκη για την προστασία της ανθρώπινης αξιοπρέπειας και κατ' επέκταση της ασφάλειας επεξεργασίας των προσωπικών τους δεδομένων, οδήγησε την Ευρωπαϊκή Ένωση (ΕΕ) να θεσπίσει την οδηγία 95/46/ΕΚ η οποία και αποτέλεσε για περίπου δύο δεκαετίες το βασικό κείμενο αναφοράς σε Ευρωπαϊκό επίπεδο για θέματα προστασίας δεδομένων προσωπικού χαρακτήρα σε όλα τα κράτη-μέλη της. Η Οδηγία αυτή όρισε σύνολο προϋποθέσεων νόμιμης επεξεργασίας προσωπικών δεδομένων και πλέον έχει αντικατασταθεί από το Γενικό Κανονισμό Προστασίας Δεδομένων.

5.2 Γενικός Κανονισμός Προστασίας Δεδομένων (ΓΚΠΔ)

Ο Γενικός Κανονισμός Προστασίας Δεδομένων-ΓΚΠΔ 2016/679 [7] του Ευρωπαϊκού Κοινοβουλίου (γνωστό και ως General Data Protection Regulation-GDPR) σε θέματα προστασίας των ατόμων για την επεξεργασία προσωπικών δεδομένων, αντικατέστησε την οδηγία 95/46/ΕΚ στις 25 Μαΐου του 2018 και στην ουσία :

- Εναρμονίζει βασικούς κανόνες μεταξύ των κρατών-μελών

- Γίνεται άμεση εφαρμογή του σε όλα τα κράτη μέλη (καταργείται η οδηγία 95/46/ΕΚ και οι εθνικές νομοθεσίες-για πολύ λίγα επιμέρους θέματα αφήνει περιθώρια στον εθνικό νομοθέτη)

- Ενισχύονται τα δικαιώματα των πολιτών

- Επιβάλλει το ύψος των «κυρώσεων» (προστίμων) που μπορούν να επιβληθούν (πολύ μεγαλύτερες κυρώσεις από ότι προέβλεπε η Οδηγία 95/46/ΕΚ)

- Ενισχύει την προστασία προσωπικών δεδομένων

5.2.1 Προσωπικά δεδομένα σύμφωνα με τον ΓΚΠΔ

Σύμφωνα με τον ΓΚΠΔ, προσωπικά δεδομένα θεωρείται κάθε πληροφορία (άμεση ή έμμεση) που μπορεί να οδηγήσει στην ταυτοποίηση ενός ατόμου (ουσιαστικά παραμένει ο ίδιος ορισμός με αυτόν που ίσχυε στην Οδηγία 95/46/ΕΚ, όπως περιγράφηκε και νωρίτερα), ενώ το πρόσωπο το οποίο αφορούν τα δεδομένα ονομάζεται «υποκείμενο» των δεδομένων» (data subject).

5.2.2 Ευαίσθητα Προσωπικά δεδομένα

Υπάρχουν κάποια προσωπικά δεδομένα που χρήζουν ακόμα μεγαλύτερης προστασίας διότι εμπίπτουν στο σκληρό πυρήνα της ιδιωτικότητας και ονομάζονται ευαίσθητα προσωπικά δεδομένα και είναι τα δεδομένα τα οποία αφορούν σε:

- Φυλετική ή εθνική προέλευση
- Πολιτικά φρονήματα
- Θρησκευτικές ή φιλοσοφικές πεποιθήσεις
- Συμμετοχή σε συνδικαλιστική οργάνωση
- Υγεία
- Κοινωνική πρόνοια
- Ερωτική ζωή
- Ποινικές διώξεις
- Γενετικά δεδομένα

- Βιομετρικά δεδομένα (εφόσον χρησιμοποιούνται για το σκοπό της ταυτοποίησης του ατόμου).

5.2.3 Ανώνυμα δεδομένα

Ανώνυμα δεδομένα ορίζονται τα δεδομένα τα οποία δεν μπορούν να συσχετιστούν με οποιονδήποτε τρόπο με ταυτοποιήσιμο πρόσωπο. Πρέπει όμως να λαμβάνονται υπόψη όλα τα μέσα (χρόνος, χρήμα, τεχνολογία) που μπορούν να χρησιμοποιηθούν από κάποιον ή κάποιους για την άμεση ή έμμεση εξακρίβωση του ατόμου, προτού χαρακτηριστούν τα δεδομένα ως ανώνυμα. Το νομικό πλαίσιο του ΓΚΠΔ δεν εφαρμόζεται σε δεδομένα που έχουν καταστεί ανώνυμα αρκεί βέβαια να έχει εκμηδενιστεί, όχι μειωθεί, η δυνατότητα ανακάλυψης της ταυτότητας του ατόμου κάτι που γίνεται συχνά λανθασμένα, με αποτέλεσμα πολλοί να θεωρούν ότι έχουν κάνει ανωνυμοποίηση σε δεδομένα χωρίς όμως να το έχουν πράγματι επιτύχει.

5.2.4 Ψευδωνυμοποιημένα δεδομένα

Ψευδωνυμοποιημένα δεδομένα θεωρούνται τα δεδομένα τα οποία έχουν υποστεί επεξεργασία ώστε να μην μπορούν να αποδοθούν σε συγκεκριμένο πρόσωπο χωρίς τη χρήση συμπληρωματικών πληροφοριών, εφόσον οι εν λόγω συμπληρωματικές πληροφορίες διατηρούνται χωριστά και υπόκεινται σε τεχνικά και οργανωτικά μέτρα. Τα ψευδωνυμοποιημένα δεδομένα δεν θεωρούνται «ανώνυμα» δεδομένα, απλά ο ΓΚΠΔ προκρίνει τη χρήση της ψευδωνυμοποίησης για περαιτέρω διασφάλιση της ασφάλειας της επεξεργασίας και της προστασίας των θεμελιωδών δικαιωμάτων. Άλλωστε ο ΓΚΠΔ αναφέρει σε πολλά σημεία του, ως κίνδυνο, την «άρση της ψευδωνυμοποίησης». Η ψευδωνυμοποίηση είναι, σύμφωνα με τον ΓΚΠΔ, ένα πολύ ευαίσθητο ζήτημα γιατί δεν πρέπει με κανέναν τρόπο ένας εισβολέας να μπορέσει να ανακαλύψει την ταυτότητα του χρήστη.

5.2.5 Βασικοί Ορισμοί

Ο ΓΚΠΔ χρησιμοποιεί κάποιους ορισμούς ώστε να διαχωρίσει τους ρόλους όλων όσων συμμετέχουν στην επεξεργασία δεδομένων:

- Επεξεργασία δεδομένων είναι η συλλογή, καταχώριση, οργάνωση, αποθήκευση, τροποποίηση, εξαγωγή, ανάκτηση, αναζήτηση, χρήση, ανακοίνωση, διαβίβαση, διασύνδεση και γενικά κάθε εργασία αυτοματοποιημένη ή μη.

- Υποκείμενο δεδομένων, ονομάζεται το φυσικό πρόσωπο το οποίο αφορούν τα δεδομένα.

- Υπεύθυνος επεξεργασίας, ονομάζεται το φυσικό ή νομικό πρόσωπο που καθορίζει το σκοπό και τον τρόπο επεξεργασίας.

- Εκτελών την επεξεργασία, ονομάζεται το φυσικό ή νομικό πρόσωπο που δρα για λογαριασμό του υπεύθυνου επεξεργασίας

5.2.6 Νομιμότητα επεξεργασίας προσωπικών δεδομένων που ορίζει ο ΓΚΠΔ

Ο ΓΚΠΔ στο άρθρο 5 [7] του, ορίζει κάποιες αρχές που πρέπει να διέπουν κάθε επεξεργασία προσωπικών δεδομένων:

- Νομιμότητα, αντικειμενικότητα και διαφάνεια

- Περιορισμός του σκοπού απόκτησης προσωπικών δεδομένων

- Ελαχιστοποίηση των δεδομένων

- Ακρίβεια

- Περιορισμός της περιόδου αποθήκευσης

- Ακεραιότητα και εμπιστευτικότητα

- Λογοδοσία

Ειδικότερα, σύμφωνα με τα ανωτέρω, τα δεδομένα που χρησιμοποιούνται ή συλλέγονται θα πρέπει να είναι τα ελάχιστα δυνατά που είναι απαραίτητα για τους σκοπούς για τους οποίους υποβάλλονται σε επεξεργασία. Θα πρέπει να είναι ακριβή ενώ οποιαδήποτε ανακριβή δεδομένα θα πρέπει να διαγράφονται και η επεξεργασία ή η συλλογή τους να γίνεται με γνώμονα τη διαφάνεια και τη δικαιοσύνη του χρήστη-υποκειμένου. Στη συνέχεια, η επεξεργασία αυτή θα

πρέπει να γίνεται για κάποιο νόμιμο σκοπό ενημερώνοντας ρητά το υποκείμενο-χρήστη και για χρονικό διάστημα τόσο όσο χρειάζεται για να εξυπηρετηθεί ο σκοπός αυτός. Και τελευταίο, αλλά πολύ σημαντικό, είναι να αναφέρουμε ότι ο υπεύθυνος επεξεργασίας φέρει την ευθύνη και πρέπει να είναι σε θέση να αποδείξει τη συμμόρφωση σε νομικές υποχρεώσεις.

Πέραν των ανωτέρω, για να είναι νόμιμη μια επεξεργασία προσωπικών δεδομένων πρέπει να συντρέχει κάποια νομική βάση, εξ αυτών που παρατίθενται στο άρθρο 6 του ΓΚΠΔ. Μια πιθανή νομική βάση για τη νομιμότητα της επεξεργασίας είναι ότι το υποκείμενο των δεδομένων, έχει δώσει τη συγκατάθεσή του με ελεύθερη, ρητή και εν πλήρει επίγνωση η οποία δίνεται με δήλωση ή σαφή ενέργεια (δηλαδή η συγκατάθεση δεν πρέπει να υπονοείται αλλά να είναι ξεκάθαρη). Υπάρχουν βέβαια περιπτώσεις στις οποίες η επεξεργασία είναι νόμιμη χωρίς τη συγκατάθεση των υποκειμένων (δηλαδή υπάρχουν και άλλες νομικές βάσεις) για παράδειγμα όταν είναι αναγκαία στο πλαίσιο σύμβασης, όταν επιβάλλεται από τον νόμο, όταν η επεξεργασία είναι αναγκαία για τη διαφύλαξη ζωτικών συμφερόντων του υποκειμένου, όταν είναι αναγκαία για την εκπλήρωση καθήκοντος για το δημόσιο συμφέρον αλλά και για την ικανοποίηση έννομου συμφέροντος του υπεύθυνου επεξεργασίας στον οποίο ανακοινώνονται τα δεδομένα και του οποίου το συμφέρον υπερέχει των δικαιωμάτων του υποκειμένου των δεδομένων.

Πρόσθετες προϋποθέσεις νομιμότητας για την επεξεργασία ευαίσθητων δεδομένων (όπως είναι τα δεδομένα υγείας) δίνονται στο άρθρο 9 του ΓΚΠΔ.

Πρέπει επίσης να σημειωθεί ότι στην ΕΕ είναι σε ισχύ και η Οδηγία 2002/58/ΕΚ (e-Privacy Οδηγία) αναφορικά με το ειδικότερο ζήτημα της προστασίας προσωπικών δεδομένων στις ηλεκτρονικές επικοινωνίες. Κάποια ειδικότερα ζητήματα λοιπόν εμπίπτουν σε αυτό το ειδικότερο νομικό πλαίσιο – όπου κάποια εξ αυτών αφορούν και την επεξεργασία δεδομένων από «έξυπνες» εφαρμογές. Ειδικότερα, σύμφωνα με την ως άνω Οδηγία, «η αποθήκευση πληροφοριών ή η απόκτηση πρόσβασης σε ήδη αποθηκευμένες πληροφορίες στον τερματικό εξοπλισμό συνδρομητή ή χρήστη επιτρέπεται μόνον εάν ο συγκεκριμένος συνδρομητής ή χρήστης έχει δώσει τη συγκατάθεσή του με βάση σαφείς και εκτενείς πληροφορίες (…), μεταξύ άλλων για το σκοπό της επεξεργασίας. Τούτο δεν εμποδίζει οιαδήποτε τεχνικής φύσεως αποθήκευση ή πρόσβαση, αποκλειστικός σκοπός της οποίας είναι η διενέργεια της διαβίβασης μιας επικοινωνίας μέσω δικτύου ηλεκτρονικών επικοινωνιών ή που είναι απολύτως αναγκαία για να μπορεί ο πάροχος υπηρεσίας της κοινωνίας της πληροφορίας την οποία έχει ζητήσει ρητά ο συνδρομητής ή ο χρήστης να παρέχει τη συγκεκριμένη υπηρεσία». Συνεπώς, η νομιμότητα των προσβάσεων σε πληροφορίες μίας έξυπνης κινητής συσκευής από μία εφαρμογή εμπίπτει κατ'

αρχάς στην e-Privacy Οδηγία – όπου βέβαια, τελικά, δεν διαφοροποιεί το ότι, κατά κανόνα, απαιτείται η συγκατάθεση του χρήστη κατόπιν αναλυτικής ενημέρωσής του .

Όσον αφορά τις «έξυπνες» εφαρμογές και τις «έξυπνες» συσκευές, προσωπικά δεδομένα [14]θεωρούνται και τα αναγνωριστικά των συσκευών διότι μπορούν να επιτρέψουν την ταυτοποίηση ενός χρήστη (εάν συνδυάζεται ενδεχομένως με άλλες πληροφορίες). Το λειτουργικό σύστημα Android, σχετίζεται με δύο αναγνωριστικά:

- Το αναγνωριστικό Android (Android ID), που είναι ένας μόνιμος αριθμός 64ων bit που δημιουργείται τυχαία.

- Το αναγνωριστικό διαφήμισης της Google (Google Advertising ID -GAID), το οποίο είναι ένα 32ψήφιο αλφαριθμητικό αναγνωριστικό το οποίο μπορεί να γίνει επαναφορά (reset) ανά πάσα στιγμή που θα το θελήσει ο χρήστης.

Άλλα αναγνωριστικά συσκευής ή δικτύου, όπως το μέσο ελέγχου πρόσβασης (MAC) και οι διευθύνσεις πρωτοκόλλου Διαδικτύου (IP), θα πρέπει επίσης να θεωρούνται προσωπικά δεδομένα.

5.3 Ευαίσθητα δεδομένα στα κεντρικοποιημένα συστήματα και ποιος τα διαχειρίζεται

Στα κεντρικοποιημένα συστήματα , ο διακομιστής έχει πρόσβαση στο όνομα και τηλέφωνο του χρήστη με το που γίνεται η εγγραφή του στον διακομιστή, έχει πρόσβαση στα ψευδώνυμα και τα αναγνωριστικά που ανταλλάσσονται μεταξύ των συσκευών και πρόσβαση στο ιστορικό των επαφών του χρήστη όταν τα «ανεβάσει» με τη συγκατάθεσή του, μιας και είναι ο διακομιστής εκείνος που υπολογίζει το σκορ κινδύνου (εκτίμηση κινδύνου έκθεσης στον ιό). Τα εν λόγω δεδομένα ουσιαστικά υφίστανται επεξεργασία για σκοπούς που άπτονται δημόσιας υγείας και σχετίζονται με άτομο του οποίου οι εν λόγω εφαρμογές επεξεργάζονται ευαίσθητα δεδομένα υγείας. Για αυτό λοιπόν το λόγο θα πρέπει η διαχείρισή του διακομιστή να γίνεται από εξουσιοδοτημένα άτομα τα οποία θα εξασφαλίσουν την προστασία του από εισβολές κακόβουλων χρηστών και θα διασφαλίζουν τη θεμιτή συλλογή και επεξεργασία των δεδομένων που διαχειρίζεται. Ο διακομιστής όμως δεν θα πρέπει να αποκαλύπτει ευαίσθητα προσωπικά δεδομένα των χρηστών ούτε να προσπαθεί να αποκαλύψει την ταυτότητά τους (τόσο των

θετικά διαγνωσμένων όσο και των επαφών τους κατά τη διαδικασία της ιχνηλάτησης) αφού κάτι τέτοιο θα παραβίαζε την αρχή της ελαχιστοποίησης των δεδομένων εν όψει του επιδιωκόμενου σκοπού. Όλες οι πληροφορίες που συλλέγει ο διακομιστής θα πρέπει να είναι οι ελάχιστες δυνατές ώστε να συμμορφώνεται με τον ΓΚΠΔ και να τις διαγράφει μετά από κάποιες μέρες που δεν θα του είναι πλέον χρήσιμες (συνήθως είναι 14 με 21 ημέρες).

5.4 Ευαίσθητα δεδομένα στα αποκεντρωμένα συστήματα και ποιος τα διαχειρίζεται

Στα αποκεντρωμένα συστήματα , ο διακομιστής δεν έχει κανένα ρόλο στην ιχνηλάτηση των επαφών των χρηστών. Δεν αποθηκεύει προσωπικά στοιχεία του χρήστη όπως το τηλέφωνο και το όνομά του και δεν γνωρίζει τα αναγνωριστικά που στέλνονται μεταξύ των συσκευών. Οι χρήστες που νοσούν, «ανεβάζουν» μαζικά και έπειτα από συγκατάθεσή τους όλα τα αναγνωριστικά με τη χρονολογία που τα έλαβαν στον διακομιστή ο οποίος τα διαγράφει αφού τα διανείμει στις υπόλοιπες εφαρμογές. Ο διακομιστής δεν συλλέγει το ιστορικό των επαφών των χρηστών αλλά συλλέγει μαζικά τα αναγνωριστικά θετικά διαγνωσμένων χρηστών γεγονός το οποίο μπορεί να προκαλέσει μη εξουσιοδοτημένη αναγνώρισή τους από εισβολείς και θα πρέπει οι εξουσιοδοτημένες αρχές να εξασφαλίσουν την προστασία του.

5.5 Κατευθυντήριες γραμμές του Συμβουλίου Προστασίας Δεδομένων

Το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων(European Data Protection Board – EDBP) [8] είναι ένας ανεξάρτητος ευρωπαϊκός οργανισμός με σκοπό τη διασφάλιση της συνεπούς εφαρμογής του Γενικού Κανονισμού Προστασίας Δεδομένων και την προώθηση της συνεργασίας μεταξύ των αρχών προστασίας δεδομένων της Ευρωπαϊκής Ένωσης. Οι κυβερνήσεις στρέφονται προς τη χρήση εφαρμογών ιχνηλάτησης επαφών, ως απάντηση για τη λύση της πανδημίας του ιού Covid-19 προκαλώντας ανησυχίες για την προστασία της ιδιωτικής ζωής των χρηστών που χρησιμοποιούν τις εφαρμογές αυτές. Το EDPB υπογραμμίζει ότι το νομικό πλαίσιο για την προστασία δεδομένων σχεδιάστηκε για να είναι ευέλικτο και να είναι σε θέση να επιτύχει την αποτελεσματική αντίδραση στην εξάπλωση της πανδημίας σε συνδυασμό με την προστασία των ανθρωπίνων δικαιωμάτων. Άλλωστε η προστασία των προσωπικών

δεδομένων είναι απαραίτητη για τη δημιουργία εμπιστοσύνης και ως εκ τούτου για την αποτελεσματικότητα των μέτρων. Ο ιός δεν γνωρίζει σύνορα ούτε εθνικότητες, οπότε και το EDPB προτείνει τη διαλειτουργικότητα των εφαρμογών ιχνηλάτησης επαφών ώστε να θεσπιστεί είτε μια κοινή εφαρμογή για όλα τα κράτη μέλη της Ευρωπαϊκής Ένωσης είτε ένα κοινό θεσμικό πλαίσιο.

Σύμφωνα με το EDPB [6], όλες οι εφαρμογές ιχνηλάτησης στηρίζονται στη διαχείριση ψευδωνύμων των προσωπικών δεδομένων των χρηστών. Αυτό περιλαμβάνει δεδομένα όπως δεδομένα υγείας, δεδομένα τηλεφώνου και ονόματα των χρηστών. Όπως υποστηρίζει το EDPB, η διαχείριση των δεδομένων θα πρέπει να γίνεται εθελοντικά από τον χρήστη μιας και οι χρήστες θα πρέπει να έχουν τον έλεγχο των δεδομένων τους αλλά και να κρατά τόσο χρονικό διάστημα όσο χρειάζεται για τους λόγους που δημιουργήθηκε η εφαρμογή και όχι παραπάνω και τα δεδομένα να διαγράφονται όταν πλέον δεν χρειάζονται. Γι' αυτό άλλωστε οι εφαρμογές διατηρούν τα δεδομένα αυτά, για διάστημα έως 21 ημέρες και θα πρέπει να απενεργοποιηθούν όταν η πανδημία πια τελειώσει.

Γενικά, η διαλειτουργικότητα [6]των εφαρμογών ιχνηλάτησης επαφών εντός του Ευρωπαϊκού Οικονομικού Χώρου, μπορεί να αυξήσει την αποτελεσματικότητα των εφαρμογών, ανεξάρτητα από την εφαρμογή που χρησιμοποιείται, και να ανιχνεύσει περισσότερες πιθανές επαφές. Θα απλοποιήσει τη χρήση, ειδικά για άτομα σε παραμεθόριες περιοχές, όταν ταξιδεύουν ή όταν εργάζονται σε θέσεις εργασίας ή περιοχές που ενδέχεται να εκτεθούν σε πολλά άτομα από άλλα κράτη μέλη (π.χ. για τον τουρισμό). Ωστόσο, δεδομένου του αυξημένου κίνδυνου προστασίας δεδομένων που προκύπτει από τη διαλειτουργικότητα, οι προγραμματιστές θα πρέπει να ελέγξουν και άλλες εναλλακτικές. Επιπλέον, όπως ισχύει για τις ίδιες τις εφαρμογές, τέτοιες λύσεις θα πρέπει να αποτελούν μέρος μιας ολοκληρωμένης στρατηγικής της δημόσιας υγείας για την καταπολέμηση της πανδημίας, συμπεριλαμβανομένων, μεταξύ άλλων, διαγνωστικών τεστ και χειροκίνητη ανίχνευση επαφών, με σκοπό τη βελτίωση της αποτελεσματικότητας εκτέλεσης των μέτρων. Το EDPB είναι ενήμερο για τις εφαρμογές ιχνηλάτησης επαφών με τις διαφορετικές προσεγγίσεις στα κράτη-μέλη και αναγνωρίζει τη δυσκολία να διασφαλιστεί η διαλειτουργικότητα των εφαρμογών αυτών, η οποία για να επιτευχθεί ίσως χρειαστεί σημαντική οικονομική βοήθεια. Στη συνέχεια, για να διασφαλιστεί η ελάχιστη ανταλλαγή και επεξεργασία δεδομένων, όπως απαιτείται από τον ΓΚΠΔ, οι προγραμματιστές των εφαρμογών ιχνηλάτησης, θα πρέπει να συμφωνήσουν για ένα κοινό πρωτόκολλο και συμβατές δομές δεδομένων. Έτσι για τις εφαρμογές που μοιράζονται ήδη ένα κοινό πλαίσιο ή τουλάχιστον την ίδια τεχνολογική βάση, η διαλειτουργικότητα μπορεί να είναι ευκολότερη από ό, τι για εκείνες

που δεν το κάνουν. Η διαλειτουργικότητα, θα οδηγήσει σε πρόσθετη επεξεργασία και αποκάλυψη δεδομένων σε πρόσθετες οντότητες. Όπως έχει προαναφερθεί, τα υποκείμενα των δεδομένων πρέπει να ενημερώνονται για τυχόν πρόσθετη επεξεργασία των προσωπικών τους δεδομένων και για τα εμπλεκόμενα μέρη. Τα υποκείμενα, (δηλαδή οι χρήστες των εφαρμογών), θα πρέπει πάντα να έχουν σαφή κατανόηση στο τι επεξεργασία υπόκεινται και πρέπει να συνεχίζουν να διατηρούν τον έλεγχο επεξεργασίας των δεδομένων τους. Το αργότερο, δηλαδή, που τα προσωπικά τους δεδομένα λαμβάνονται από τον προγραμματιστή, θα πρέπει να τους δοθούν σαφείς πληροφορίες σχετικά με την πρόσθετη επεξεργασία που σχετίζεται με τη χρήση της διαλειτουργικότητας. Σε αυτό το σημείο, το υποκείμενο πρέπει να ενημερωθεί για τις συνθήκες και την έκταση της επεξεργασίας των δεδομένων του.

Σε νομικό επίπεδο, οι ίδιες νομικές βάσεις με αυτές που αναφέρονται στις Οδηγίες 04/2020 του Ευρωπαϊκού Συμβουλίου Προστασίας Δεδομένων[6] εξακολουθούν να ισχύουν και εδώ. Όταν βασίζεται στο δημόσιο συμφέρον, η εθνική νομοθεσία μπορεί να χρειαστεί να προσαρμοστεί ώστε να προβλέπει την ανταλλαγή δεδομένων με άλλες υπηρεσίες. Σε περίπτωση συγκατάθεσης, θα πρέπει να συλλεχθεί μια πρόσθετη συγκατάθεση για τη διαλειτουργικότητα-επεξεργασία που πληροί όλες τις απαιτήσεις της. Όμως, όταν χρησιμοποιούνται διαφορετικές νομικές βάσεις από τους διαφορετικούς υπευθύνους επεξεργασίας δεδομένων των εφαρμογών ιχνηλάτησης επαφών, ενδέχεται να απαιτούνται πρόσθετα μέτρα για την εφαρμογή των δικαιωμάτων του υποκειμένου των δεδομένων που σχετίζονται με τη νομική βάση. Όπου η επεξεργασία αφορά τα δεδομένα υγείας, ο ΓΚΠΔ ισχύει και οι προγραμματιστές πρέπει να μπορούν να βασίζονται σε μία από τις εξαιρέσεις που αναφέρονται εκεί (στο άρθρο 9[1] αυτού).

Σύμφωνα με το EDPB, θα πρέπει να υπάρχει μια οριστική δήλωση σχετικά με τους ρόλους των εμπλεκόμενων μερών της επεξεργασίας δεδομένων του υποκειμένου και μια εκτίμηση σε πραγματική βάση για το πώς αυτή πραγματοποιείται κατά τον σχεδιασμό της λειτουργικότητας. Κατά τη γνώμη του EDPB, κάθε πράξη ή σύνολο πράξεων που επιδιώκουν τον σκοπό της διασφάλισης της διαλειτουργικότητας εκτός από την επεξεργασία της λειτουργικότητας των εφαρμογών σε κάθε κράτος-μέλος, πρέπει να αξιολογείται ξεχωριστά από προηγούμενες ή μεταγενέστερες εργασίες επεξεργασίας λόγω του πρόσθετου σκοπού. Επομένως, αυτή η πρόσθετη επεξεργασία πρέπει να θεωρηθεί ως ξεχωριστή επεξεργασία. Για αυτή την ξεχωριστή διαδικασία επεξεργασίας, τα μέρη μπορεί να είναι μεμονωμένα ή από κοινού υπεύθυνοι επεξεργασίας. Οποιαδήποτε μεταγενέστερη επεξεργασία πραγματοποιείται μετά την ανταλλαγή

[1] Το άρθρο 9 αναφέρει την επεξεργασία ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα

των αναγνωριστικών (υπολογισμός της έκθεσης, ειδοποίηση αναγνωρισμένων επαφών, κ.λπ.) θα συνέβαινε υπό ξεχωριστό έλεγχο από τον πάροχο της εφαρμογής. Οι αντίστοιχοι ρόλοι, σχέσεις και ευθύνες των κοινών υπεύθυνων επεξεργασίας, όσον αφορά τα δεδομένα, θα πρέπει να καθοριστούν και αυτές οι πληροφορίες θα πρέπει στη συνέχεια να διατεθούν στο υποκείμενο των δεδομένων. Αυτό θα έχει αντίκτυπο στο πεδίο εφαρμογής του DPIA που πρέπει να εκτελεστεί, συμπεριλαμβανομένης της επεξεργασίας που πραγματοποιείται με σκοπό τη διαλειτουργικότητα. Η επεξεργασία με σκοπό τη διασφάλιση της διαλειτουργικότητας από τρίτες οντότητες μπορεί να ανατεθεί στον υπεύθυνο επεξεργασίας που πληροί τις προϋποθέσεις του Άρθρου 28[2] του ΓΚΠΔ.

Οποιαδήποτε διαλειτουργική λύση πρέπει να διευκολύνει τον τρόπο με τον οποίο τα υποκείμενα των δεδομένων μπορούν να ασκήσουν τα δικαιώματά τους. Όπου η άσκηση των δικαιωμάτων είναι δυνατή, δεν θα πρέπει να γίνει πιο δυσκίνητη για τα υποκείμενα των δεδομένων και αυτό πρέπει να είναι σαφές σε ποιον πρέπει να στραφούν για να ασκήσουν τα δικαιώματά τους. Η παροχή πληροφοριών και ελέγχου στα υποκείμενα των δεδομένων θα αυξήσει την εμπιστοσύνη τους στις λύσεις και τις δυνατότητές της.

5.5.1 Χρήση της τοποθεσίας

Υπάρχουν δύο κύριες πηγές δεδομένων θέσης διαθέσιμων για μοντελοποίηση της εξάπλωσης του ιού και τη συνολική αποτελεσματικότητα των μέτρων περιορισμού:

- δεδομένα τοποθεσίας που συλλέγονται από παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών (όπως κινητή συσκευή ,τηλεπικοινωνιακοί φορείς) κατά τη διάρκεια της παροχής της υπηρεσίας τους και

- δεδομένα τοποθεσίας που συλλέγονται από τις εφαρμογές παρόχων υπηρεσιών της κοινωνίας της πληροφορίας των οποίων η λειτουργικότητα απαιτεί τη χρήση τέτοιων δεδομένων (π.χ. πλοήγηση, υπηρεσίες μεταφοράς και τα λοιπά).

Το EDPB[8], υπενθυμίζει ότι τα δεδομένα τοποθεσίας που συλλέγονται από παρόχους ηλεκτρονικών επικοινωνιών ενέχονται επεξεργασία μόνο εντός των αρμοδιοτήτων των άρθρων 6[3] και 9[4] της οδηγίας για την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών

[2] Το άρθρο 28 αναφέρει τις ευθύνες του εκτελούντος την επεξεργασία
[3] Άρθρο 6:Traffic Data, Άρθρο 9 Location data other than traffic data

επικοινωνιών (Οδηγία 202/58/ΕΚ/-ePrivacy). Αυτό σημαίνει ότι αυτά τα δεδομένα μπορούν να διαβιβαστούν μόνο σε αρχές ή σε τρίτους, εάν έχουν ανωνυμοποιηθεί από τον πάροχο ή για δεδομένα που δείχνουν τη γεωγραφική θέση του τερματικού ενός χρήστη, που δεν είναι δεδομένα κίνησης, με την προηγούμενη συγκατάθεση των χρηστών. Όσον αφορά τις πληροφορίες, συμπεριλαμβανομένων των δεδομένων τοποθεσίας, που συλλέγονται απευθείας από το τερματικό του χρήστη ισχύει το άρθρο 5 της οδηγίας «ePrivacy». Ως εκ τούτου, η αποθήκευση πληροφοριών σχετικά με τη συσκευή του χρήστη ή η πρόσβαση στις πληροφορίες που έχουν ήδη αποθηκευτεί επιτρέπεται μόνο εάν ο χρήστης έχει δώσει τη συγκατάθεσή του ή η αποθήκευση ή / και η πρόσβαση είναι απολύτως απαραίτητη για τις πληροφορίες που ζητήθηκε ρητά από αυτόν. Όσον αφορά την επαναχρησιμοποίηση δεδομένων τοποθεσίας που συλλέγονται από έναν πάροχο υπηρεσιών της κοινωνίας της πληροφορίας για σκοπούς μοντελοποίησης (π.χ. μέσω του λειτουργικού συστήματος ή ορισμένων που είχαν εγκατασταθεί προηγουμένως), πρέπει να πληρούνται πρόσθετοι όροι. Πράγματι, όταν έχουν συλλεχθεί δεδομένα σύμφωνα με το άρθρο 5 της ePrivacy οδηγίας για την ηλεκτρονική ιδιωτικότητα, μπορούν να υποστούν περαιτέρω επεξεργασία μόνο με τη πρόσθετη συγκατάθεση του υποκειμένου των δεδομένων ή βάσει της νομοθεσίας της Ένωσης ή των κρατών μελών η οποία πρέπει να αποτελεί απαραίτητο και αναλογικό μέτρο σε μια δημοκρατική κοινωνία για τη διασφάλιση των στόχων που αναφέρονται στο άρθρο 23 του ΓΚΠΔ.

Σύμφωνα με το EDPB [8], έμφαση πρέπει να δίνεται στα δεδομένα τοποθεσίας που είναι ανώνυμα και όχι στα προσωπικά δεδομένα. Όταν αναφερόμαστε σε ανώνυμα δεδομένα, εννοούμε τα δεδομένα που με οποιαδήποτε μέσα τεχνικά ή μη δεν θα είναι εφικτή η αποκάλυψη των πραγματικών δεδομένων του χρήστη. Αν για κάποιο λόγο τα ανώνυμα δεδομένα αποκαλύψουν οποιαδήποτε στοιχείο της ταυτότητας του χρήστη, τότε αντιτίθεται στους ορισμούς του ΓΚΠΔ και παύουν να είναι ανώνυμα. Μάλιστα ένας μεγάλος αριθμός ερευνών έχει δείξει ότι τα δεδομένα τοποθεσίας που θεωρούνται ανώνυμα, στην πραγματικότητα δεν είναι.

Η αξιολόγηση της ανθεκτικότητας της ανωνυμοποίησης βασίζεται σε τρία κριτήρια: (i) singling-out (απομόνωση) ένα άτομο σε μια μεγαλύτερη ομάδα με βάση τα δεδομένα), (ii) δυνατότητα σύνδεσης (σύνδεση δύο εγγραφών σχετικά με το ίδιο άτομο) και (iii) συμπεράσματα (συμπερασματικά, με σημαντική πιθανότητα, άγνωστες πληροφορίες για ένα άτομο).

Η έννοια της ανωνυμοποίησης είναι επιρρεπής σε παρανόηση και συχνά θεωρείται λάθος ως «ψευδωνυμοποίηση». Ενώ η ανωνυμοποίηση επιτρέπει τη χρήση των δεδομένων χωρίς κανένα περιορισμό, τα ψευδωνυμοποιημένα δεδομένα εξακολουθούν να εμπίπτουν στο πεδίο εφαρμογής του ΓΚΠΔ. Υπάρχουν πολλές επιλογές για αποτελεσματική ανωνυμοποίηση, αλλά με προειδοποίηση. Δεν είναι δυνατή η ανωνυμία των δεδομένων μεμονωμένα, που σημαίνει ότι μόνο τα σύνολα δεδομένων στο σύνολό τους μπορούν ή όχι να γίνουν ανώνυμα. Με αυτήν την έννοια, οποιαδήποτε παρέμβαση σε ένα μοτίβο δεδομένων (μέσω κρυπτογράφησης ή οποιουδήποτε άλλου μαθηματικού μετασχηματισμού), μπορεί στην καλύτερη περίπτωση να θεωρηθεί ψευδώνυμο. Οι διαδικασίες ανωνυμοποίησης και οι επιθέσεις επαναπροσδιορισμού είναι ενεργά πεδία έρευνας. Είναι κρίσιμο για κάθε υπεύθυνο επεξεργασίας που εφαρμόζει λύσεις ανωνυμοποίησης για την παρακολούθηση των πρόσφατων εξελίξεων στο αυτό το πεδίο, ειδικά όσον αφορά τα δεδομένα τοποθεσίας (που προέρχονται από φορείς εκμετάλλευσης τηλεπικοινωνιών ή / και υπηρεσίες πληροφορίας της κοινωνίας) που είναι γνωστό ότι είναι εξαιρετικά δύσκολο να ανωνυμοποιηθούν. Πράγματι, ένας μεγάλος αριθμός ερευνών έχει δείξει ότι τα δεδομένα τοποθεσίας που πιστεύεται ότι είναι ανώνυμα στην πραγματικότητα δεν είναι. Τα ίχνη κινητικότητας των ατόμων είναι εγγενώς πολύ συσχετισμένα και μοναδικά. Επομένως, υπό ορισμένες συνθήκες, μπορεί να είναι ευάλωτα σε προσπάθειες επαναπροσδιορισμού. Ένα μοτίβο δεδομένων που εντοπίζει τη θέση ενός ατόμου για μια σημαντική χρονική περίοδο δεν μπορεί να ανωνυμοποιηθεί πλήρως. Αυτό μπορεί να ισχύει ακόμη και αν δεν γίνεται με μεγάλη ακρίβεια η καταγραφή των γεωγραφικών συντεταγμένων του υποκειμένου και ακόμα κι αν διατηρείται μόνο η τοποθεσία των τόπων όπου το υποκείμενο των δεδομένων παραμένει για σημαντικό χρονικό διάστημα. Για να επιτευχθεί ανωνυμοποίηση, τα δεδομένα τοποθεσίας πρέπει να υποβληθούν σε προσεκτική επεξεργασία, προκειμένου να ανταποκριθούν στο τεστ λογικής. Υπό αυτήν την έννοια, μια τέτοια επεξεργασία περιλαμβάνει την εξέταση του συνόλου των δεδομένων τοποθεσίας ως ολόκληρο, καθώς και την επεξεργασία δεδομένων από ένα αρκετά μεγάλο σύνολο ατόμων που χρησιμοποιούν ισχυρές τεχνικές ανωνυμοποίησης, υπό τον όρο ότι είναι επαρκώς και αποτελεσματικά εφαρμόσιμες. Τέλος, δεδομένης της πολυπλοκότητας των διαδικασιών ανωνυμοποίησης, η διαφάνεια όσον αφορά τη μεθοδολογία ανωνυμοποίησης ενθαρρύνεται ιδιαίτερα.

5.5.2 Νομική Βάση συστημάτων ιχνηλάτησης

Η συστηματική παρακολούθηση της θέσης και των επαφών των ατόμων είναι στην πραγματικότητα επέμβαση στην ιδιωτική τους ζωή. Αν όμως γίνει με τη συγκατάθεσή τους τότε τα πράγματα αλλάζουν. Αυτό συνεπάγεται, ότι τα άτομα που αποφασίζουν να μην χρησιμοποιούν εφαρμογές δεν πρέπει να τιμωρηθούν. Για να διασφαλιστεί η λογοδοσία, ο υπεύθυνος επεξεργασίας οποιασδήποτε εφαρμογής ανίχνευσης επαφών πρέπει να είναι σαφής και να ορίζεται. Σύμφωνα με το EDPB [8]καλύτερα θα ήταν ως υπεύθυνοι επεξεργασίας αυτών των εφαρμογών να είναι οι επίσημες υγειονομικές αρχές και να ορίζονται ρητά και ξεκάθαρα στους χρήστες οι ρόλοι και οι ευθύνες του καθενός. Τα δεδομένα που χρησιμοποιούνται θα πρέπει να είναι τα λιγότερα δυνατά που χρειάζονται ώστε να επιτευχθεί ο σκοπός δημιουργίας των εφαρμογών αυτών και να αποκλειστεί περαιτέρω επεξεργασία για σκοπούς που δεν σχετίζονται με την αντιμετώπιση της πανδημίας. Άρα δεν θα πρέπει οι εφαρμογές

- Να λειτουργούν ως αναγνώριση των χρηστών και θα πρέπει να θεσπιστούν κατάλληλα μέτρα για την αποφυγή του επαναπροσδιορισμού

- Να χρησιμοποιούνται για παρακολούθηση της τοποθεσίας των χρηστών, αλλά να χρησιμοποιούνται δεδομένα εγγύτητας

- Να συλλέγουν δεδομένα όταν δεν χρειάζονται και αυτά πρέπει να βρίσκονται στο τερματικό των χρηστών

- Να συλλέγουν επιπλέον προσωπικά δεδομένα των χρηστών

- Να συλλέγουν δεδομένα χωρίς τη συγκατάθεση των χρηστών

- Να στηρίζονται στη συγκατάθεση των χρηστών για να επεξεργαστούν επιπλέον δεδομένα και ιδίως για αυτά που βρίσκονται ήδη στο τερματικό τους

Τα προσωπικά δεδομένα θα πρέπει να διατηρούνται μόνο για τη διάρκεια της κρίσης COVID-19. έπειτα, κατά γενικό κανόνα, όλα τα προσωπικά δεδομένα πρέπει να διαγραφούν ή να ανωνυμοποιηθούν. Προκειμένου να διασφαλιστεί η ορθότητά τους και γενικότερα, η συμμόρφωσή τους με τους νόμους, οι αλγόριθμοι ιχνηλάτησης πρέπει να ελέγχονται τακτικά από ανεξάρτητους εμπειρογνώμονες και ο πηγαίος κώδικας της εφαρμογής θα πρέπει να διατίθεται στο κοινό για όσο το δυνατόν λεπτομερέστερο έλεγχο.

Επειδή οι εφαρμογές αυτές είναι εφαρμογές αντιμετώπισης της πανδημίας και στην ουσία και πρωταρχικά διαχειρίζονται δεδομένα υγείας (την κατάσταση ενός μολυσμένου ατόμου), η επεξεργασία αυτών των δεδομένων υγείας θα πρέπει να γίνεται μόνο για λόγους έρευνας, για στατιστικούς λόγους και για λόγους απαραίτητους για τη δημόσια υγεία και για το δημόσιο συμφέρον.

Οι εφαρμογές αυτές δεν δύναται να αντικαταστήσουν το εξειδικευμένο προσωπικό υγείας αλλά μόνο να στηρίξουν τη δύσκολη διαδικασία ιχνηλάτησης των επαφών μιας και οι επαφές μπορεί ή μπορεί και όχι να οδηγήσουν στη μετάδοση του ιού. Μη λησμονούμε άλλωστε ότι τα άτομα από ντροπή ή και από απροσεξία δεν δύναται να αποκαλύψουν όλες τις επαφές τους στο εξειδικευμένο προσωπικό υγείας, οπότε οι εφαρμογές αυτές αποσκοπούν μόνο να στηρίξουν αυτή την προσπάθεια ιχνηλάτησης τους. Επιπλέον οι εφαρμογές θα πρέπει να επιβλέπονται από εξουσιοδοτημένο και εξειδικευμένο προσωπικό προκειμένου να περιοριστεί όσο το δυνατόν η εμφάνιση λανθασμένων θετικών και αρνητικών κρουσμάτων γιατί κάτι τέτοιο θα επιφέρει την πτώση του συστήματος ιχνηλάτησης. Βέβαια, λανθασμένα θετικά αποτελέσματα θα υπάρχουν ως κάποιο βαθμό και επειδή αυτά ως επακόλουθο θα έχουν την απομόνωση των ατόμων-χρηστών μέχρι να κάνουν τεστ και να βγουν αρνητικά, είναι απαραίτητη η δυνατότητα διόρθωσης των δεδομένων από κάποιο εξουσιοδοτημένο πρόσωπο. Τέλος, θα πρέπει να πραγματοποιηθεί μια εκτίμηση επιπτώσεων στην προστασία δεδομένων προτού μια τέτοια εφαρμογή δοθεί στο κοινό ώστε να είναι προετοιμασμένοι οι προγραμματιστές και οι υγειονομικές αρχές από κάθε είδους απειλή – εισβολή που θα μπορούσε να υπάρξει και να έχει ως αποτέλεσμα την έλλειψη εμπιστοσύνης των χρηστών και συνεπώς την κατάρρευση του συστήματος. Η εκτίμηση επιπτώσεων προβλέπεται στο άρθρο 35 του ΓΚΠΔ ως υποχρεωτική για έναν υπεύθυνο επεξεργασίας σε περιπτώσεις όπου η επεξεργασία ενέχει πολλούς κινδύνους για τα δικαιώματα και τις ελευθερίες των υποκειμένων.

5.5.3 Συστάσεις και λειτουργικές απαιτήσεις

Όπως προαναφέρθηκε και προηγουμένως, τα δεδομένα που συλλέγονται πρέπει να μην επιτρέπουν τη δυνατότητα αναγνώρισης του χρήστη και να είναι τα λιγότερα δυνατά για το σκοπό δημιουργίας της εφαρμογής ιχνηλάτησης. Τα ανώνυμα δεδομένα αναφέρονται στα μοναδικά και κρυπτογραφημένα αναγνωριστικά τα οποία πρέπει να ανανεώνονται τακτικά ώστε να εξυπηρετούν τόσο την ανωνυμοποίηση όσο και την επαρκή παρακολούθηση των επαφών για την εξάπλωση του ιού.

Οι εφαρμογές είτε ακολουθούν το κεντρικοποιημένο είτε το αποκεντρωμένο σύστημα πρέπει να θεωρούνται βιώσιμες επιλογές, αρκεί να υπάρχουν επαρκή μέτρα προστασίας, μιας και το κάθε ένα περιλαμβάνει ένα σύνολο από πλεονεκτήματα και μειονεκτήματα στην προστασία των προσωπικών δεδομένων και στην εξυπηρέτηση του σκοπού δημιουργίας τους τα οποία και θα πρέπει να ληφθούν υπόψη πριν από τη δημιουργία τους.

Κάθε διακομιστής που εμπλέκεται στο σύστημα ιχνηλάτησης των επαφών, θα πρέπει να συλλέγει μόνο το ιστορικό των επαφών των μολυσμένων ατόμων ή το κρυπτογραφημένο αναγνωριστικό τους και όχι μη συμβατές με το σκοπό αυτό πληροφορίες όπως καταγραφή μηνυμάτων και κλήσεων και πάντα κάθε συλλογή πρέπει να γίνεται με τη ρητή συγκατάθεση του χρήστη. Ο διακομιστής δεν θα πρέπει επίσης να προσπαθήσει να εντοπίσει τους δυνητικά μολυσμένους χρήστες παρά μόνο να υλοποιήσει ένα σκορ κινδύνου και απλά να τους ειδοποιήσει ώστε να απομονωθούν ή να τους προτρέψει να πάνε να κάνουν ένα διαγνωστικό τεστ.

Όπως προαναφέρθηκε, τα αναγνωριστικά θα πρέπει να κρυπτογραφούνται και ειδικά να χρησιμοποιούνται προηγμένες τεχνικές κρυπτογραφίας για την προστασία δεδομένων που είναι αποθηκευμένα σε διακομιστή και εφαρμογές όπως επίσης και να προηγηθεί πιστοποίηση της αυθεντικότητας μεταξύ εφαρμογής και διακομιστή.

Επίσης πολύ σημαντικό είναι να αναφερθεί η πιστοποίηση της αυθεντικότητας του θετικά διαγνωσμένου χρήστη με κάποιον τρόπο είτε μέσω κωδικού μιας χρήσης είτε με μοναδικό σειριακό αριθμό που υπάρχει στο τεστ ενός εξουσιοδοτημένου διαγνωστικού κέντρου. Η επεξεργασία των δεδομένων του χρήστη θα πρέπει να γίνεται μόνο εάν προηγηθεί πιστοποίηση της αυθεντικότητας του θετικά διαγνωσμένου χρήστη ώστε να αποφευχθεί κάθε είδους εισβολή προς το σύστημα και σε λανθασμένα αποτελέσματα. Τέλος θα πρέπει οι υγειονομικές αρχές να ενημερώνουν τους χρήστες για την επίσημη εθνική εφαρμογή ώστε να μετριαστεί ο κίνδυνος να χρησιμοποιήσουν τα άτομα εφαρμογές από τρίτες και συνεπώς κακόβουλες οντότητες.

5.5.4 Συνοψίζοντας- Ορισμοί

- **Επαφή:** Θεωρείται ο οποιοσδήποτε έχει έρθει τόσο κοντά σε ένα θετικά διαγνωσμένο άτομο που να υπάρχει ο κίνδυνος να έχει κολλήσει και αυτός. Το πόσο κοντά εξαρτάται από τον εκάστοτε υγειονομικό φορέα (για παράδειγμα απόσταση μικρότερη του 1,5 μέτρου και για διάστημα περίπου 10 λεπτών).

- **Δεδομένα Τοποθεσίας:** Περιλαμβάνει το γεωγραφικό μήκος και πλάτος της κινητής συσκευής του χρήστη, την κατεύθυνση που αυτός κινείται και τον χρόνο τον οποίο καταγράφηκαν τα δεδομένα.

- **Επαφή Ιχνηλάτησης:** Αναφέρεται στην ιχνηλάτηση των επαφών θετικά διαγνωσμένων ατόμων ώστε να ελεγχθεί η εξάπλωση της πανδημίας με το να ελεγχθούν εάν βρίσκονται σε κίνδυνο μόλυνσης και να παρθούν τα κατάλληλα μέτρα.

- **Αλληλεπίδραση:** Αναφέρεται στην ανταλλαγή αναγνωριστικών μεταξύ δύο κοντινών συσκευών μέσω μιας τεχνολογίας επικοινωνιών πχ BLE

- **Φορέας Ιού:** Αναφέρονται στους χρήστες- άτομα που έχουν διαγνωστεί θετικά από ένα εξουσιοδοτημένο ιατρικό διαγνωστικό κέντρο.

Συνοψίζοντας λοιπόν οι εφαρμογές ιχνηλάτησης θα πρέπει να συλλέγουν δεδομένα μόνο κατά την περίοδο του ιού και μετά να διαγράφονται. Τα δεδομένα να είναι μόνο αυτά που είναι χρήσιμα για την ιχνηλάτηση των επαφών και όχι προσωπικά δεδομένα του χρήστη. Ο σκοπός τους δεν είναι η αποκάλυψη των χρηστών που νοσούν αλλά η σωστή ιχνηλάτηση των επαφών των θετικά διαγνωσμένων ατόμων από επίσημο υγειονομικό φορέα. Ο κώδικας των εφαρμογών θα πρέπει να είναι ανοιχτός προς το κοινό το οποίο θα ενημερώνεται ρητά και ξεκάθαρα ότι μόνο με τη συγκατάθεσή του θα συλλέγονται τα δεδομένα και ποιος είναι ο σκοπός επεξεργασίας τους. Οι χρήστες που είναι σε κίνδυνο έκθεσης στον ιό θα ενημερώνονται από την εφαρμογή η οποία θα υπολογίσει ένα σκορ κινδύνου ανάλογα με την απόσταση και τον χρόνο που έχει έρθει σε επαφή με νοσούν άτομο. Οι εφαρμογές θα πρέπει να στηρίζουν τη διαλειτουργικότητα εντός της Ευρωπαϊκής Ένωσης. Θα πρέπει να μεταδίδουν κρυπτογραφημένα αναγνωριστικά σε τακτά χρονικά διαστήματα και η μετάδοση αυτών να στηρίζεται στο BLE . Οι εφαρμογές μπορούν να στηρίζονται σε κεντρικοποιημένα ή αποκεντρικοποιημένα συστήματα στα οποία η επικοινωνία με τον διακομιστή θα πρέπει να γίνεται μέσω έμπιστου καναλιού ώστε να μην αποκαλύπτονται πληροφορίες σε τρίτες οντότητες. Τέλος θα πρέπει να γίνεται πιστοποίηση της αυθεντικότητας τόσο της εφαρμογής με τον διακομιστή όσο και του χρήστη με την εφαρμογή και πρόσβαση στα δεδομένα του χρήστη να έχουν μόνο εξουσιοδοτημένοι φορείς.

Κεφάλαιο 6

Μελέτη εφαρμογών σε πρακτικό περιβάλλον

Στο παρόν κεφάλαιο, αφού έχουν ήδη μελετηθεί οι πιο γνωστές εφαρμογές ιχνηλάτησης κρουσμάτων COVID-19 ως προς τα σχεδιαστικά τους χαρακτηριστικά, καθώς επίσης και οι συναφείς κίνδυνοι που ελλοχεύουν για την ιδιωτικότητα των χρηστών, θα εστιάσουμε στη μελέτη βασικών εφαρμογών αυτής της κατηγορίας σε πειραματικό περιβάλλον, προκειμένου να διερευνηθούν, με κατάλληλα εργαλεία λογισμικού, οι υποκείμενες επεξεργασίες δεδομένων που λαμβάνουν χώρα από τις εφαρμογές αυτές –υπό το πρίσμα και των γενικών κινδύνων ιδιωτικότητας από «έξυπνες» εφαρμογές κάθε κατηγορίας, τις οποίες συζητήσαμε στο Κεφάλαιο 5.

6.1 Εγκατάσταση Εικονικού Περιβάλλοντος

Το Φεβρουάριο του 2019, ο οργανισμός «Privacy International»[17], κυκλοφόρησε το περιβάλλον παρακολούθησης δεδομένων για τη διερεύνηση εφαρμογών και για τον έλεγχο της λειτουργίας τους. Το ίδιο περιβάλλον χρησιμοποιήθηκε για τις αλληλεπιδράσεις εφαρμογών με το Facebook στο Android 5, όπου δημοσιεύθηκαν ενδιαφέροντα αποτελέσματα. Το προαναφερθέν περιβάλλον, εγκαταστάθηκε και διαμορφώθηκε για τα ερευνητικά μας πειράματα σε εικονικό περιβάλλον. Αρχικά επισκεπτόμαστε τη διεύθυνση https://privacyinternational.org/node/2732#prerequisites-as-this-is-a-quick-start-guide και κατεβάζουμε το Privacy-International-data-interception-environment-stable-2.1.2.ova το οποίο και θα είναι το εικονικό περιβάλλον στο οποίο θα δουλέψουμε. Για τη δημιουργία του περιβάλλοντος δοκιμών θα χρησιμοποιήσουμε τα εξής:

- Έναν υπολογιστή windows 10 με 8gb ram
- Ένα oracle virtual VM manager box 6.1
- Privacy-International-data-interception-environment-stable-2.1.2.ova
- Usb WiFi adapter Ralink 5370
- Μια κινητή συσκευή με λειτουργικό android 6 (samsung A3)
- Μια κινητή συσκευή με λειτουργικό android 5(blackview A8)
- Μια κινητή συσκευή με λειτουργικό android 10(realme)

Virtualbox (6.0.4)

Το Virtualbox είναι ένας δωρεάν διαχειριστής εικονικής μηχανής πολλαπλών πλατφόρμων. Επιτρέπει τη λειτουργία ενός λειτουργικού συστήματος εντός ενός άλλου, μιμούμενος τα χαρακτηριστικά ενός φυσικού υπολογιστή.

Debian 10 (Buster)

Το Debian μια διανομή του GNU / Linux, ενός πυρήνα τύπου UNIX και της αρχιτεκτονικής του λειτουργικού συστήματος.

mitmproxy (4.0.4)

Το mitmproxy είναι ένας διακομιστής μεσολάβησης ανοιχτού κώδικα γραμμένος στην Python. Στην ουσία, δέχεται συνδέσεις από τη μία πλευρά, τις «διαβάζει» και στη συνέχεια τις προωθεί στην άλλη πλευρά. Το βασικό χαρακτηριστικό του είναι ότι δημιουργεί απαιτούμενα πιστοποιητικά σε πραγματικό χρόνο καταφέρνοντας έτσι να αναλύσει και κρυπτογραφημένες συνδέσεις. Αυτό διασφαλίζει ότι η εισερχόμενη σύνδεση (από τον πελάτη), πιστεύει ότι ο διακομιστής μεσολάβησης είναι ο πραγματικός προορισμός. Σε αυτό το προκαθορισμένο περιβάλλον, το mitmproxy διαμορφώνεται σε "διαφανή" λειτουργία. Αυτό σημαίνει ότι δεν χρειάζεται να αλλαχθούν οι ρυθμίσεις στον πελάτη, εκτός από την εγκατάσταση του πιστοποιητικού του mitmproxy.

dnsmasq (2.80) (Ενεργοποιημένο)

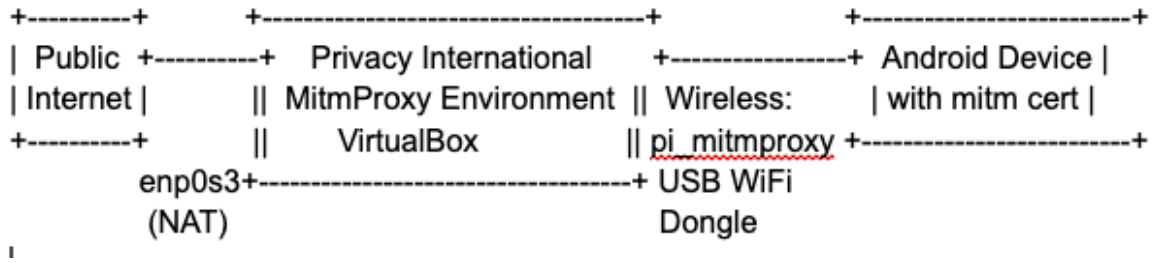
Το dnsmasq είναι ένας διακομιστής DNS (υπηρεσία ονόματος τομέα) και DHCP (πρωτόκολλο διαμόρφωσης δυναμικού κεντρικού υπολογιστή). Εξυπηρετεί δύο σκοπούς, πρώτον δίνει διευθύνσεις IP επιτρέποντας έτσι σε συσκευές να ενταχθούν σε ένα δεδομένο δίκτυο χωρίς να χρειάζεται να διαμορφωθούν χειροκίνητα ρυθμίσεις για συγκεκριμένα δίκτυα όπως η προεπιλεγμένη διαδρομή και ο τομέας και δεύτερον παρέχει αιτήματα DNS. Αυτό περιλαμβάνει κυρίως τη μετατροπή ονομάτων τομέα όπως privacyinternational.org σε διευθύνσεις IP όπως η 144.76.205.68.

hostapd (2.6) (Απενεργοποιημένο)

Το hostapd είναι ένα δίκτυο 802.11 (ασύρματο LAN), το οποίο επιτρέπει τη διαμόρφωση ασύρματων συσκευών με διάφορους τρόπους. Σε αυτό το σύνολο εργαλείων, είναι απενεργοποιημένο από προεπιλογή. Ωστόσο, έχει μια προεπιλεγμένη λογική διαμόρφωση και μπορεί εύκολα να ενεργοποιηθεί.

iptables (1.8.2)

Το iptables είναι το τυπικό σύστημα τείχους προστασίας σε πολλά λειτουργικά συστήματα που βασίζονται σε Linux. Χρησιμοποιεί έναν πίνακα κανόνων, αναγνώσιμων από τον άνθρωπο για την κατηγοριοποίηση και τον χειρισμό της κυκλοφορίας μέσω ενός συνόλου γνωστών καταστάσεων δικτύωσης. Σε αυτό το σύνολο εργαλείων εξυπηρετεί δύο σκοπούς, τροφοδοτεί την κίνηση από τις θύρες 80 (http) και 443 (https) σε mitmproxy και επιτρέπει επίσης τη μεταμφίεση (masqueraded) άλλων συνδέσεων έτσι ώστε το VM να λειτουργεί σαν δρομολογητής.



ΕΙΚΌΝΑ 8:ΣΥΝΔΕΣΗ ΔΙΚΤΥΟΥ

Διάταξη στοιχείου

- Το Διαδίκτυο όπως φαίνεται στην Εικόνα 8 μπορεί να είναι κάθε πρόσβαση από/προς αυτό, με όποιον τρόπο κι αν συνήθως συνδέεται κάποιος στο διαδίκτυο.

- Ο προσαρμογέας 1 στο εικονικό πλαίσιο (enp0s3 μέσα στο VM) πρέπει να οριστεί ως συσκευή NAT. Αυτό σημαίνει ότι η VM θα χρησιμοποιήσει τη σύνδεση δικτύου του κεντρικού

(host) υπολογιστή για να αποκτήσει πρόσβαση στο Διαδίκτυο χωρίς να απαιτείται καμία άλλη ρύθμιση εντός της εικονικής μηχανής.

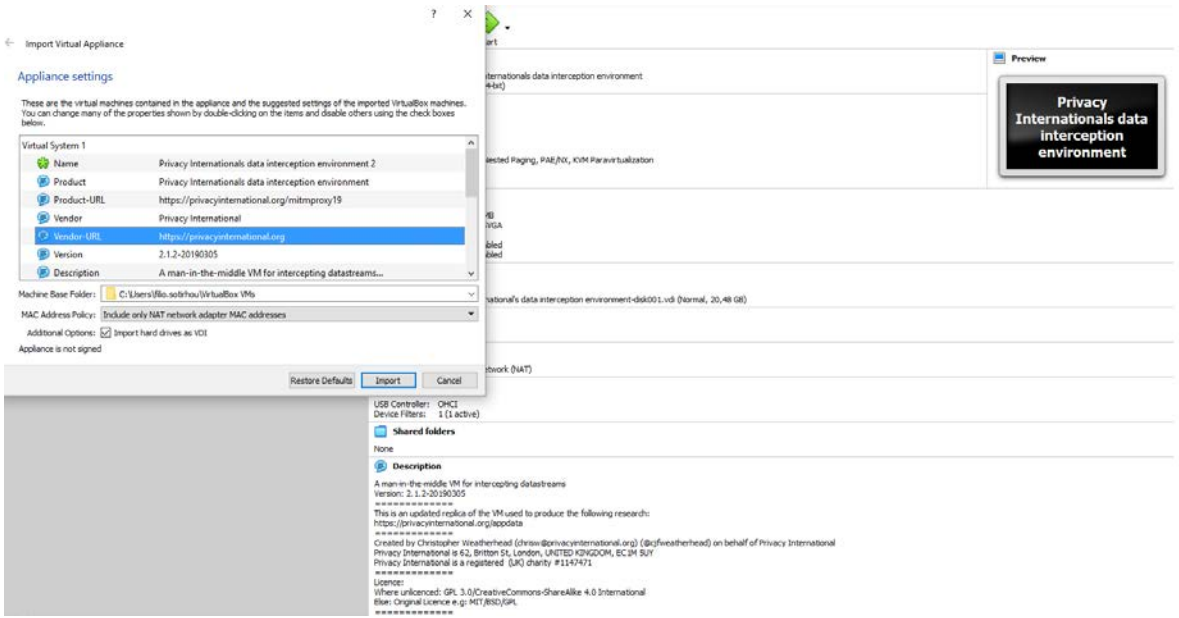
- Η VM πρέπει να ξεκινήσει και το mitmproxy πρέπει να εκτελείται από την αρχή προτού προσπαθήσει κανείς να συνδέσει τυχόν συσκευές.

- Στα δεξιά του VM υπάρχει ένα ασύρματο NIC (υποθέτουμε ένα USB dongle). Αυτό πρέπει να ρυθμιστεί προτού επιχειρήσει κάποιος να εκτελέσει το mitmproxy. Θα φιλοξενήσει το ασύρματο δίκτυο pi_maninthemiddle.

- Τέλος, στην δεξιά πλευρά βρίσκεται η συσκευή Android την οποία θα αναλύσουμε. Πρέπει να συνδεθεί στο δίκτυο που παρέχεται από το WLAN NIC (pi_mitmproxy) και πρέπει να έχει εγκατασταθεί το πιστοποιητικό mitmproxy στο σύστημα της συσκευής.

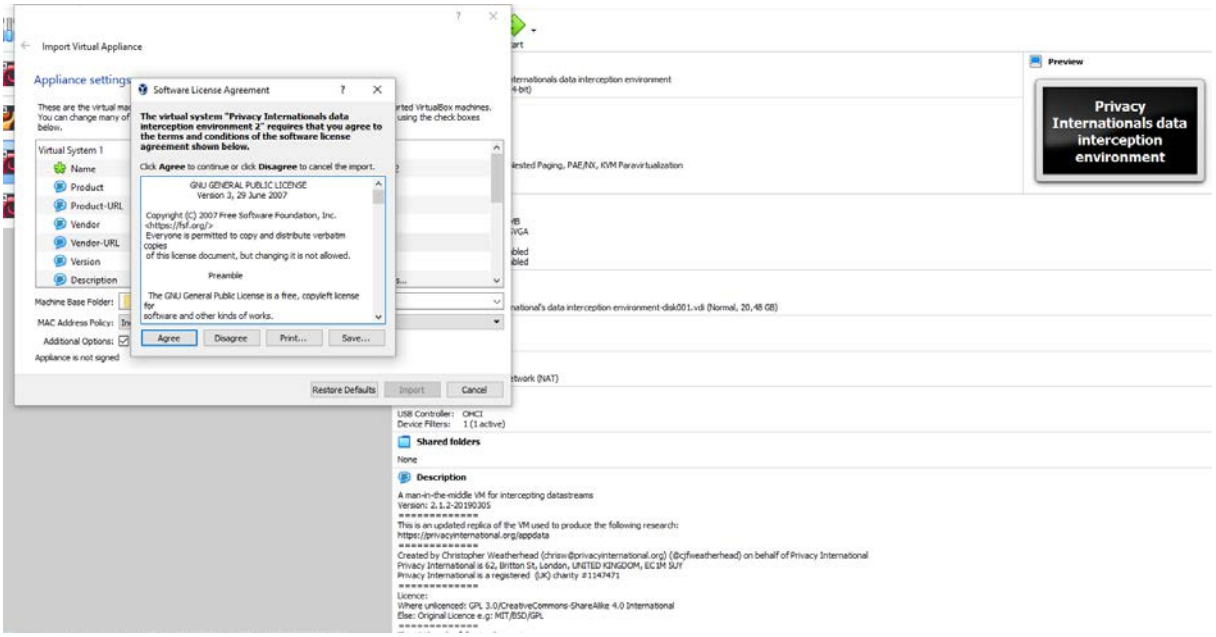
6.1.1 Διαδικασία Εγκατάστασης

Εγκαθιστούμε το oracle virtual VM manager box στο φορητό υπολογιστή με λειτουργικό σύστημα Windows 10. Βρίσκουμε το εικονικό περιβάλλον που κατεβάσαμε (**Privacy-International-data-interception-environment-stable-2.1.2.ova)** και πατώντας επάνω του με διπλό κλικ ανοίγει αυτόματα το virtual box όπως φαίνεται στην Εικόνα 9.



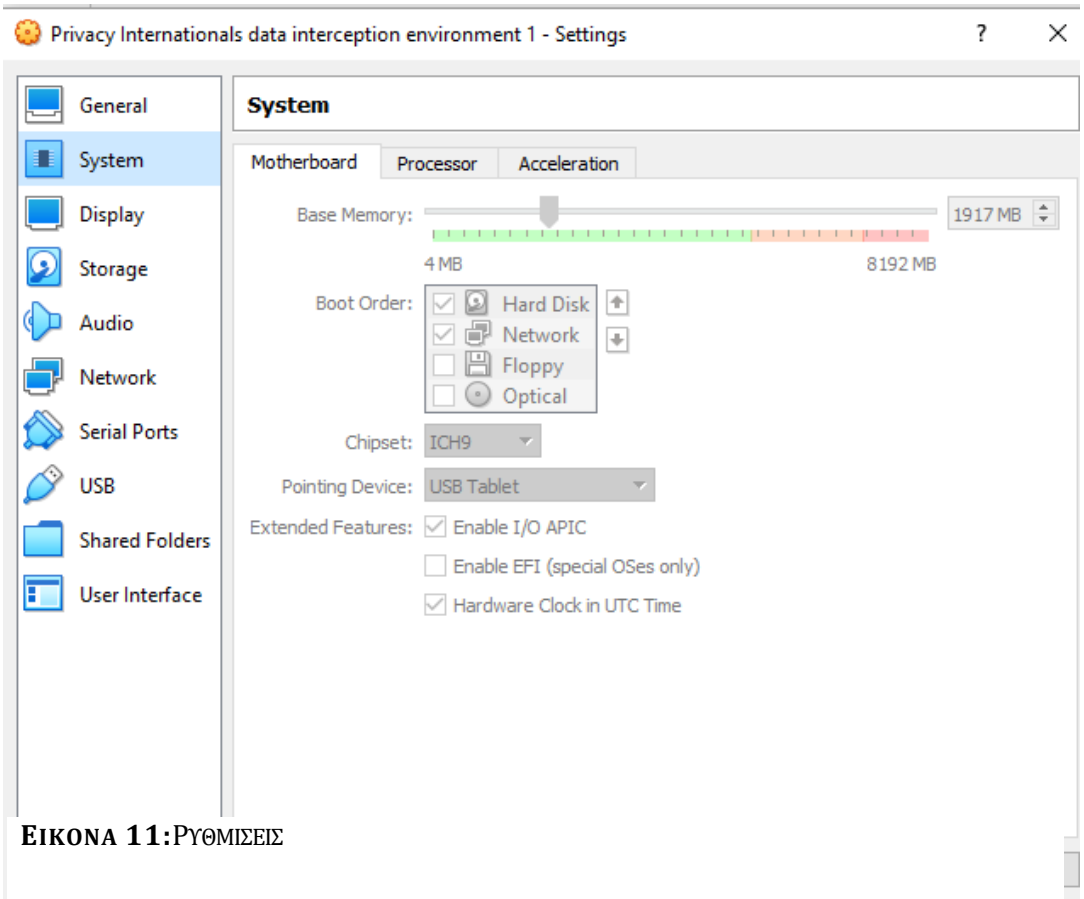
ΕΙΚΟΝΑ 9: ΕΓΚΑΤΑΣΤΑΣΗ ΕΙΚΟΝΙΚΟΥ ΠΕΡΙΒΑΛΛΟΝΤΟΣ

Επιλέγοντας στη συνέχεια “import” και “agree”, τοποθετείται αυτόματα μέσα στο oracle virtual VM manager box όπως φαίνεται και στην Εικόνα 10.



ΕΙΚΟΝΑ 10 : ΕΓΚΑΤΑΣΤΑΣΗ ΕΙΚΟΝΙΚΟΥ ΠΕΡΙΒΑΛΛΟΝΤΟΣ

Εκεί κάνουμε τις απαραίτητες ενέργειες, αλλάζουμε δηλαδή τις ρυθμίσεις ώστε η μνήμη να είναι τουλάχιστον 1917 MB, το usb ralink 802.11 να είναι συνδεδεμένο στο «usb» (βλ Εικόνα 11).



ΕΙΚΟΝΑ 11: ΡΥΘΜΙΣΕΙΣ

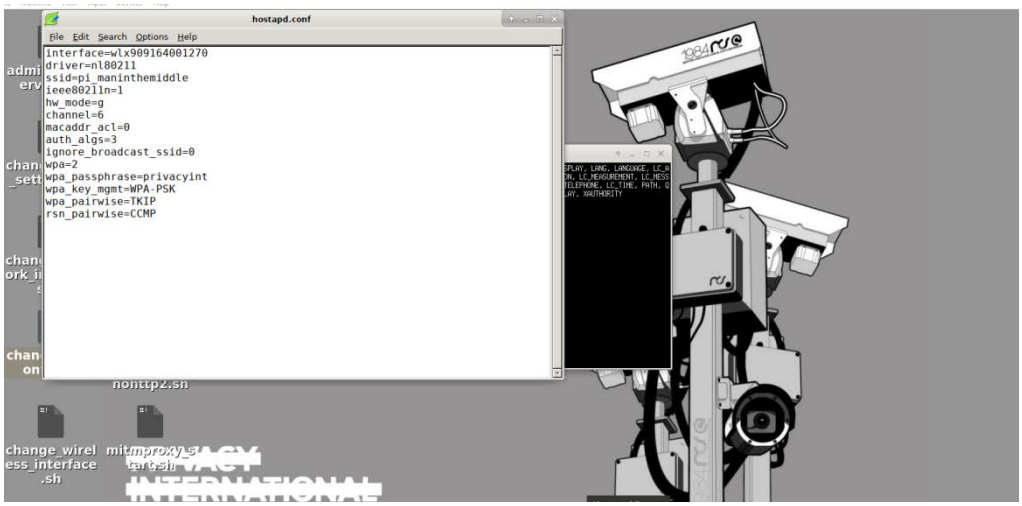
Και πατάμε εκκίνηση να «φορτώσει» το εικονικό μας περιβάλλον όπως φαίνεται και παρακάτω (βλ Εικόνα 12).

ΕΙΚΌΝΑ 12: ΕΙΚΟΝΙΚΟ ΠΕΡΙΒΑΛΛΟΝ

Στην επιφάνεια εργασίας υπάρχουν κάποια αρχεία που θα χρειαστεί να τροποποιήσουμε. Αρχικά είναι το change_wireless_interface.sh το οποίο αφού το εκτελέσουμε, εμφανίζεται ένα παράθυρο και αφού διαλέξουμε την επιλογή "Execute in terminal" , εμφανίζεται ένα ακόμα παράθυρο το οποίο μας ενημερώνει ότι το wireless nic που χρησιμοποιούμε έχει interface wlx909164001270 όπως φαίνεται στην Εικόνα 13 και θέλουμε να ενημερώσει το «configuration» αρχείο. Αποδεχόμαστε την επιλογή και κλείνει μόνο του.

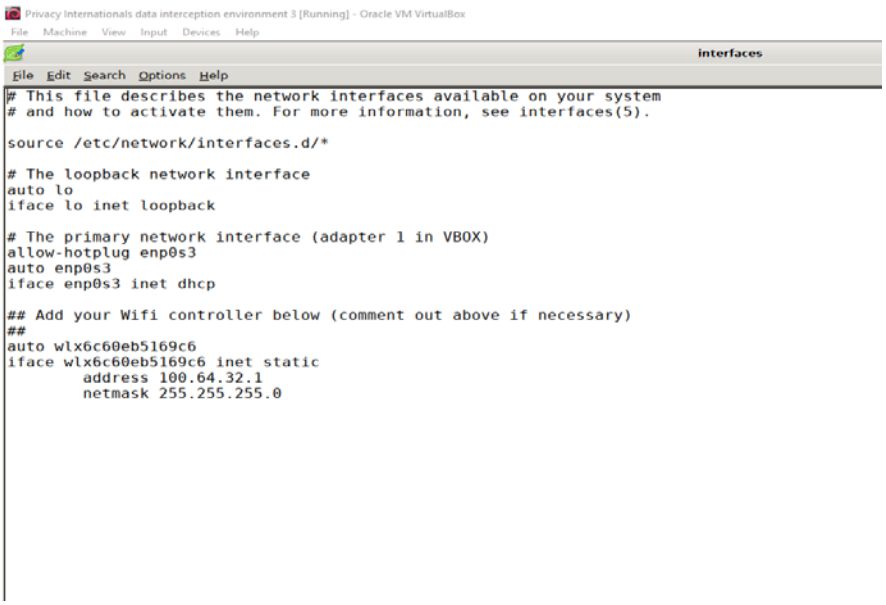
ΕΙΚΌΝΑ 13: EXECUTE CHANGE_WIRELESS_INTERFACE.SH

Στη συνέχεια ανοίγουμε το αρχείο «change_wificonfig.sh"(βλ Εικόνα 14) με τον ίδιο τρόπο όπως πριν, το οποίο στην ουσία αποτελεί το hostapd αρχείο που χρειάζεται να τροποποιήσουμε για να συνδεθούμε. Αρχικά βάζουμε το interface του nic wlx909164001270, τον driver=nl80211 ενώ το ssid και το password το αφήνουμε ως έχει (αν θέλουμε τα αλλάζουμε). Προσθέτουμε και το ieee80211n=1 γιατί το nic είναι 802.11n και αποθηκεύουμε.



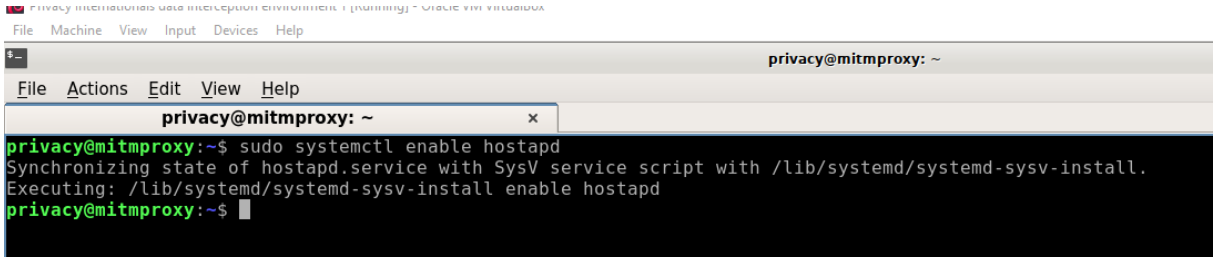
ΕΙΚΌΝΑ 14: HOSTAPD

Τέλος εκτελούμε και το αρχείο change_network_interface.sh το οποίο είναι στην ουσία το interface του nic που χρησιμοποιούμε βλ Εικόνα 15 :



ΕΙΚΌΝΑ 15: WIRELESS INTERFACE

Βγάζουμε από τα σχόλια το WiFi controller, και βάζουμε το σωστό interface “wlx909164001270” , βάζουμε τη διεύθυνση που θέλουμε να «ακούει» το nic εδώ τη 100.64.32.1 και τη μάσκα υποδικτύου 255.255.255.0 και αποθηκεύουμε. Στη συνέχεια για να «τρέξουμε» το hostapad, ανοίγουμε το applications < system tools < Qterminal και γράφουμε την εντολή “sudo systemctl enable hostapd”, όπως φαίνεται στην εικόνα 16 και παίρνουμε το ακόλουθο αποτέλεσμα:



ΕΙΚΌΝΑ 16: EXECUTE HOSTAPD

Στη συνέχεια ανοίγουμε το Qterminal και πληκτρολογούμε τις εντολές: “sudo service dnsmasq restart” για να αποθηκευτούν οι αλλαγές που κάναμε στο dnsmasq προηγουμένως και ”sudo service networking restart” για να γίνει επανεκκίνηση στα interfaces.

Αν πατήσουμε την εντολή “sudo iw wlx909164001270 info” μας βγάζει όλες τις πληροφορίες για τα interfaces που διαθέτουμε. Αφού εμφανιστεί το “pi_maninthemiddle”, πατάμε πάνω να συνδεθούμε, βάζουμε τον κωδικό που τον έχουμε στο hostapd.conf και ο οποίος είναι “privacyint” και συνδεόμαστε στο δίκτυο. Παρατηρούμε ότι μας επισημαίνει ότι «δεν έχει σύνδεση στο διαδίκτυο» το οποίο και περιμέναμε. Πληκτρολογούμε τη διεύθυνση http://mitm.it και μας βγάζει τα πιστοποιητικά και «κατεβάζουμε» εκείνο που είναι για android όπως φαίνεται στην εικόνα 17.

ΕΙΚΌΝΑ 17: ΠΙΣΤΟΠΟΙΗΤΙΚΟ MITMPROXY

Στη συνέχεια για να το εγκαταστήσουμε σε μία κινητή συσκευή με λειτουργικό android 5, πηγαίνουμε στις ρυθμίσεις→ασφάλεια→εγκατάσταση πιστοποιητικών από το χώρο αποθήκευσης.

Για να εγκαταστήσουμε το πιστοποιητικό σε android 7 **και πάνω** , αφού αποκτήσουμε root πρόσβαση στην κινητή συσκευή, πληκτρολογούμε τις εξής εντολές στο Qterminal :

- sudo openssl x509 -inform PEM -subject_hash_old -in /root/.mitmproxy/mitmproxy-ca-cert.pem | head -1 η οποία μας δίνει το όνομα του πιστοποιητικού c8750f0d
- adb push /root/.mitmproxy/mitmproxy-ca-cert.pem /sdcard/< c8750f0d.0 όπου αντιγράφουμε το πιστοποιητικό στην κινητή συσκευή μέσω adb και στη συνέχεια δίνουμε πρόσβαση στο πιστοποιητικό να είναι read/write. Προσοχή χρειάζεται να είμαστε root.
- adb shell
- su
- mount -o remount,rw /system
- cp /sdcard/<NamefromOpenSSLOutput>.0 /system/etc/security/cacerts
- chmod 644 /system/etc/security/cacerts/NamefromOpenSSLOutput>.0
- chown root:root /system/etc/security/cacerts/NamefromOpenSSLOutput>.0
- mount -o remount,ro /system και μετά κάνουμε επανεκκίνηση τη συσκευή

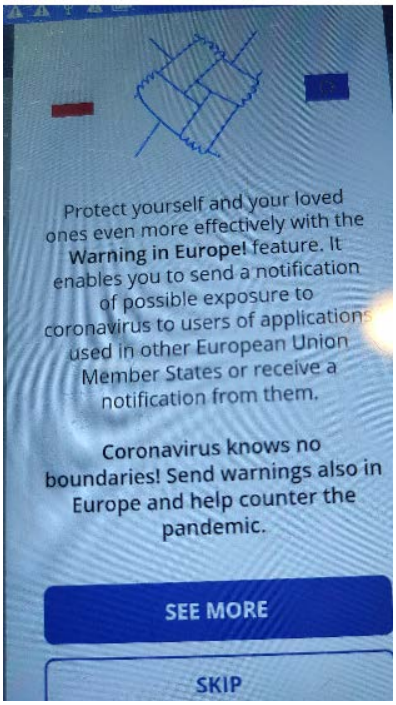
6.2 Ανάλυση Εφαρμογών ιχνηλάτησης

Στο πλαίσιο της παρούσης διατριβής, μελετήσαμε στο ως άνω πειραματικό περιβάλλον κάποιες από τις πιο γνωστές εφαρμογές ιχνηλάτησης, τόσο στην Ευρώπη όσο και στον υπόλοιπο κόσμο

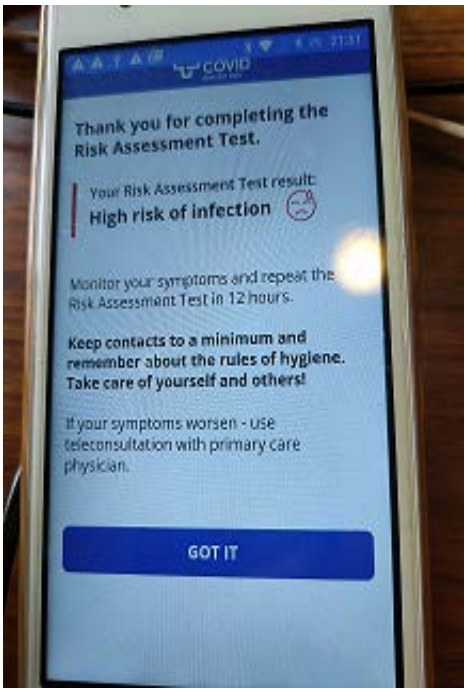
και μάλιστα από όλες τις κατηγορίες συστημάτων ιχνηλάτησης, (κεντρικοποιημένα ή μη και για τις διάφορες δυνατές προσεγγίσεις υλοποίησης).

6.2.1 STOP COVID - ProteGO Safe

Μεταβαίνουμε στο play store και «κατεβάζουμε» την πρώτη εφαρμογή που θα ελέγξουμε και είναι η STOP COVID - ProteGO Safe, χρησιμοποιώντας ένα blackview A8 με έκδοση λειτουργικού android 5. Η εφαρμογή STOP COVID - ProteGO Safe είναι μια εφαρμογή της Πολωνίας η οποία βασίζεται στο αποκεντρωμένο σύστημα. Παρατηρούμε ότι δεν χρειάζεται εγγραφή σε διακομιστή, παρά μόνο ένα ψευδώνυμο και το σκορ κινδύνου γίνεται τοπικά στην εφαρμογή (βλ Εικόνα 19) όπως σε όλες τις εφαρμογές που στηρίζονται σε αποκεντρωμένα συστήματα. Στηρίζει τη διαλειτουργικότητα (βλ Εικόνα 18)μιας και δουλεύει η εφαρμογή σε οποιαδήποτε χώρα εντός της Ε.Ε.



Εικόνα 18: ΔΙΑΛΕΙΤΟΥΡΓΙΚΟΤΗΤΑ ΕΦΑΡΜΟΓΗΣ

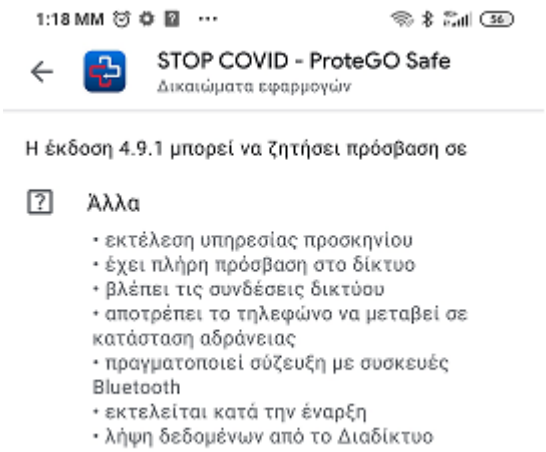


Εικόνα 19: ΣΚΟΡ ΚΙΝΔΥΝΟΥ

Η εφαρμογή ενημερώνει το χρήστη για το πώς δουλεύει, ότι στέλνει κρυπτογραφημένα αναγνωριστικά σε κοντινές συσκευές μέσω BLE και για αυτό του τονίζει ότι το BLE πρέπει να

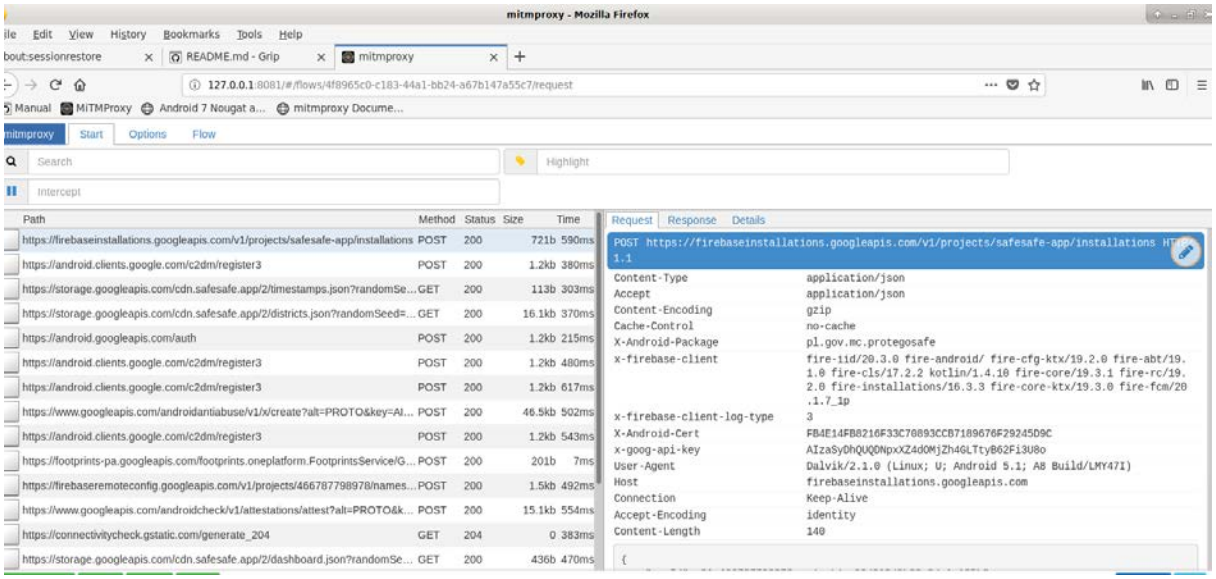
είναι ανοιχτό. Του δίνει την επιλογή εάν έχει κάνει τεστ από διαγνωσμένο κέντρο να το προσθέσει ώστε να ειδοποιηθούν οι επαφές του. Δίνει τη δυνατότητα στον χρήστη να προσθέσει ένα προσωπικό ημερολόγιο για να παρακολουθεί τη υγεία του αλλά και να σημειώνει με ποιους ήρθε σε επαφή βάσει του Παγκόσμιου Οργανισμού Υγείας (ΠΟΥ) και τέλος τον ενημερώνει ότι τα δεδομένα του θα αποθηκεύονται για 2 μόνο εβδομάδες.

Δεν ζητάει περαιτέρω αποδοχή σε πρόσβαση στα συστήματα της κινητής συσκευής, παρά μόνο τα κάτωθι (βλ. Εικόνα 20), όπως φαίνονται στις πληροφορίες της εφαρμογής στο Google Play Store.

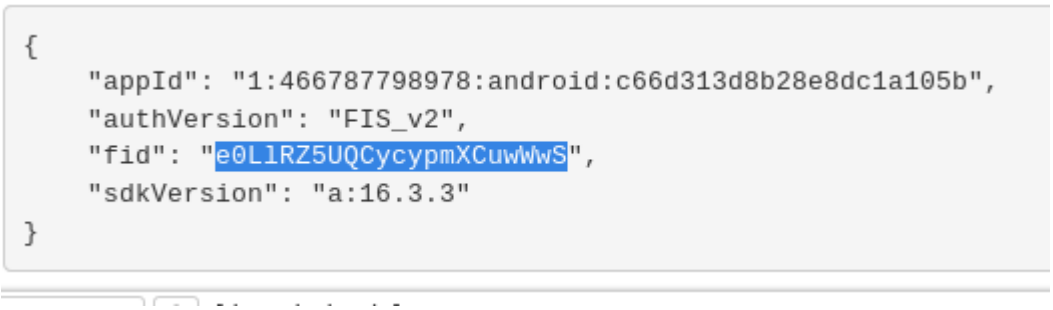


ΕΙΚΟΝΑ 20: ΔΙΚΑΙΩΜΑΤΑ ΕΦΑΡΜΟΓΗΣ

Ανοίγουμε την εφαρμογή, διαλέγουμε τη γλώσσα και τρέχουμε το mitmproxy_start.sh και κάνουμε διάφορες δοκιμές για 320 δευτερόλεπτα (βλ. Εικόνα 21).

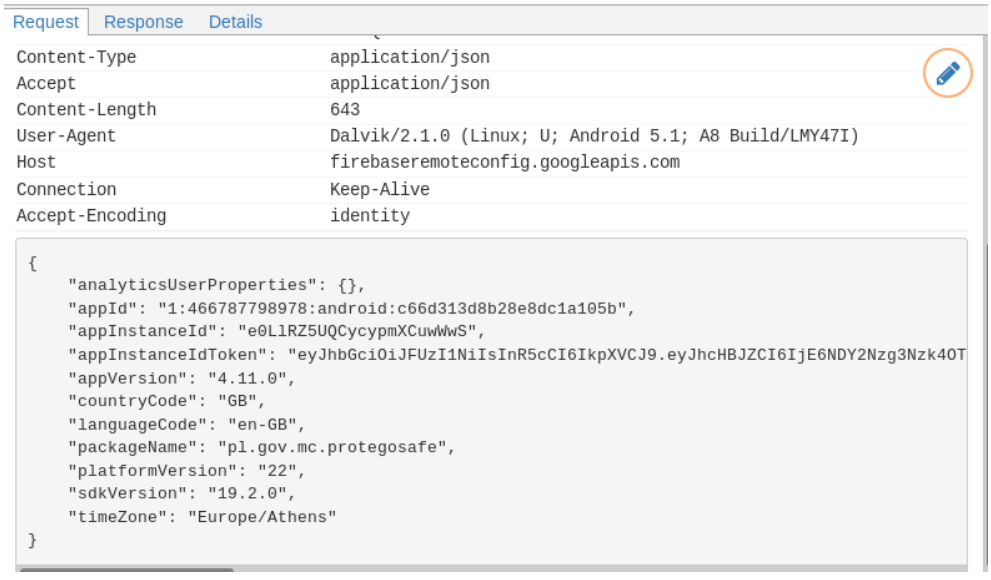


ΕΙΚΌΝΑ 21: ΣΤΙΓΜΙΟΤΥΠΟ ΜΕ MITMPROXY



ΕΙΚΟΝΑ 22:FIREBASE

Με το που εγκαταστήσαμε την εφαρμογή, διαπιστώνουμε ότι συνδέθηκε με την υπηρεσία Google Firebase. Η Google έχει πρόσβαση σε όλα τα δεδομένα που μεταδίδονται από την εφαρμογή μέσω της Firebase. Το "fid": " e0LlRZ5UQCycypmXCuwWwS" είναι το αναγνωριστικό της Firebase (Firebase instance ID) το οποίο αναγνωρίζει την τωρινή κατάσταση της εφαρμογής (βλ Εικόνα 22). Η απάντηση για το «αίτημα» αυτό, είναι δύο token(authToken, refreshToken) τα οποία σε συνδυασμό με το fid και κάτι που μοιάζει με αναγνωριστικό της συσκευής(name =), αποστέλλονται στη Google. Στη συνέχεια, κάνει αιτήματα προς τη "firebaseremoteconfig" αποκαλύπτοντας τη χώρα που βάλαμε στο τηλέφωνο, τη ζώνη ώρας «Europe/Athens» (βλ. Εικόνα 22). Το αναγνωριστικό της εφαρμογής (appID=1:466787798978…),το αναγνωριστικό της τωρινής κατάστασής της (appInstance ID= e0LlRZ5UQCycypmXCuwWwS…), τη γλώσσα που έχουμε βάλει στη συσκευή και την έκδοση της εφαρμογής,



ΕΙΚΟΝΑ 22:ΑΠΟΤΕΛΕΣΜΑΤΑ PROTEGO SAFE ΤΗΣ FIREBASE

Όπως προαναφέραμε και βλέπουμε και παρακάτω, το fid,token, android αποστέλλονται στην Google(βλ Εικόνα 23 και 24).

```
POST https://android.clients.google.com/c2dm/register3 HTTP/1.1
Authorization          AidLogin 3699243521003246695:5855884455874054178
app                    pl.gov.mc.protegosafe
gcm_ver                17785008
User-Agent             Android-GCM/1.5 (A8 LMY47I)
content-length         1188
content-type           application/x-www-form-urlencoded
Host                   android.clients.google.com
Connection             Keep-Alive
Accept-Encoding        identity
```

ΕΙΚΟΝΑ 23: ΕΥΡΗΜΑΤΑ ANDROID.CLIENTS.GOOGLE

Request Response Details

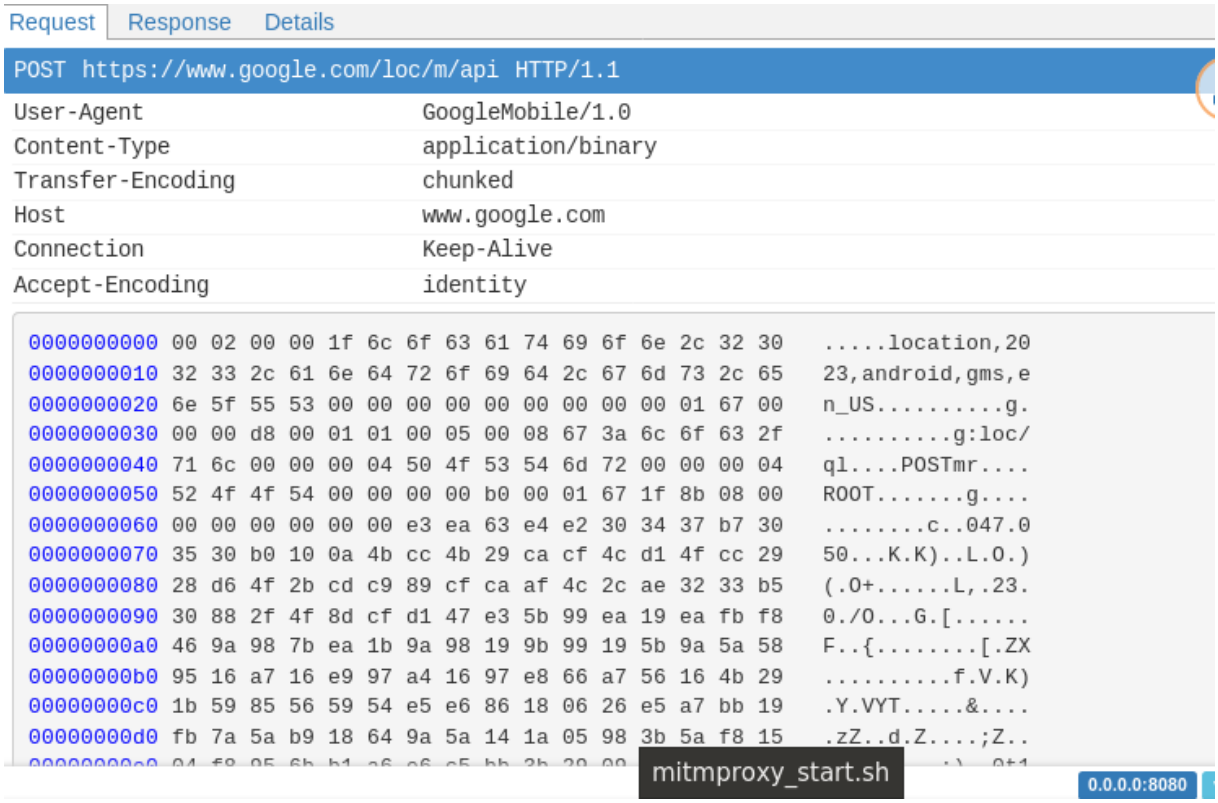
```
X-subtype:                          466787798978
sender:                             466787798978
X-app_ver:                          89
X-osv:                              22
X-cliv:                             fiid-20.3.0
X-gmsv:                             17785008
X-appid:                            e0LlRZ5UQCycypmXCuwWwS
X-scope:                            *
X-Goog-Firebase-Installations-Auth:eyJhbGciOiJFUzI1NiIsInR5cCI6IkpXVCJ9.eyJhcHBJZCI6IjE6NDY2Nz
X-gmp_app_id:                       1:466787798978:android:c66d313d8b28e8dc1a105b
X-Firebase-Client:                  fire-iid/20.3.0 fire-android/ fire-cfg-ktx/19.2.0 fire-abt/19.
X-firebase-app-name-hash:           R1dAH9Ui7M-ynoznwBdw01tLxhI
X-Firebase-Client-Log-Type:         1
X-app_ver_name:                     4.11.0
app:                                pl.gov.mc.protegosafe
device:                             3699243521003246695
app_ver:                            89
info:                               Ix1RJhSWyi8YsHCPESFjClUb6o__vRU
gcm_ver:                            17785008
plat:                               0
cert:                               fb4e14fb8216f33c70893ccb7189676f29245d9c
target_ver:                         29
```

ΕΙΚΟΝΑ 24: ΕΥΡΗΜΑΤΑ FID,TOKEN,ANDROID

Στην εικόνα 25, φαίνεται το αμέσως επόμενο «αίτημα» της εφαρμογής προς το «mihome2» και παρατηρούμε ότι αποκαλύπτονται στοιχεία για το μοντέλο της κινητής συσκευής, το λογισμικό της, την οθόνη της ακόμα και το build number(A8_BLACKVIEW_V0.9_2016.05.19) και ο σειριακός αριθμός της συσκευής «SERIAL NUMBER 0123456789ABCDEF).

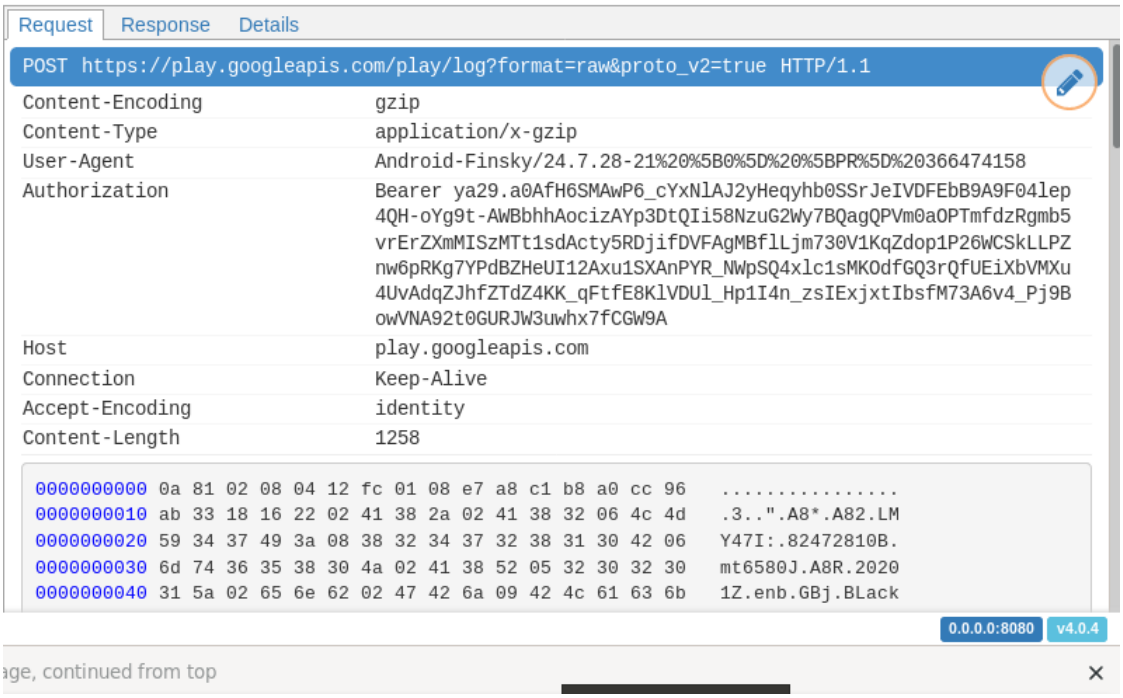
ΕΙΚΟΝΑ 25:ΑΠΟΤΕΛΕΣΜΑΤΑ PROTEGO SAFEΠΡΟΣ MIHOME2.COM

Οι περισσότερες [5] από τις εφαρμογές που υπάρχουν, χρησιμοποιούν την υπηρεσία έκθεσης των Google/ Apple, οπότε και αποκαλύπτουν στην Google δεδομένα τα οποία δεν μπορούν να αποφευχθούν εκτός και αν απενεργοποιηθούν οι υπηρεσίες του Google Play. Το γεγονός ότι οι υπηρεσίες του Google Play συνδέονται τακτικά με τους διακομιστές της Google, αποκαλύπτουν την (handset)IP διεύθυνση, η οποία είναι ένας διακομιστής μεσολάβησης για την τοποθεσία του χρήστη, το οποίο αναφέρεται και στο έγγραφο πολιτικής της Google όπως επίσης και στην τεκμηρίωση της Firebase SDK ότι δεν χρειάζεται ένας προγραμματιστής να γράψει επιπλέον κώδικα για τη συλλογή ορισμένων ιδιοτήτων του χρήστη και ότι το Analytics δίνει δεδομένα τοποθεσίας προερχόμενα από τις IP διευθύνσεις των χρηστών. Η εφαρμογή ProteGo SAFE , εκτός από τα «αιτήματα» που κάνει προς τη Firebase, παρατηρούμε ότι κάνει αιτήματα προς την google.com/loc, της μορφής όπως φαίνονται παρακάτω (βλ εικόνα 26) αποκαλύπτοντας τη διεύθυνσή μας.



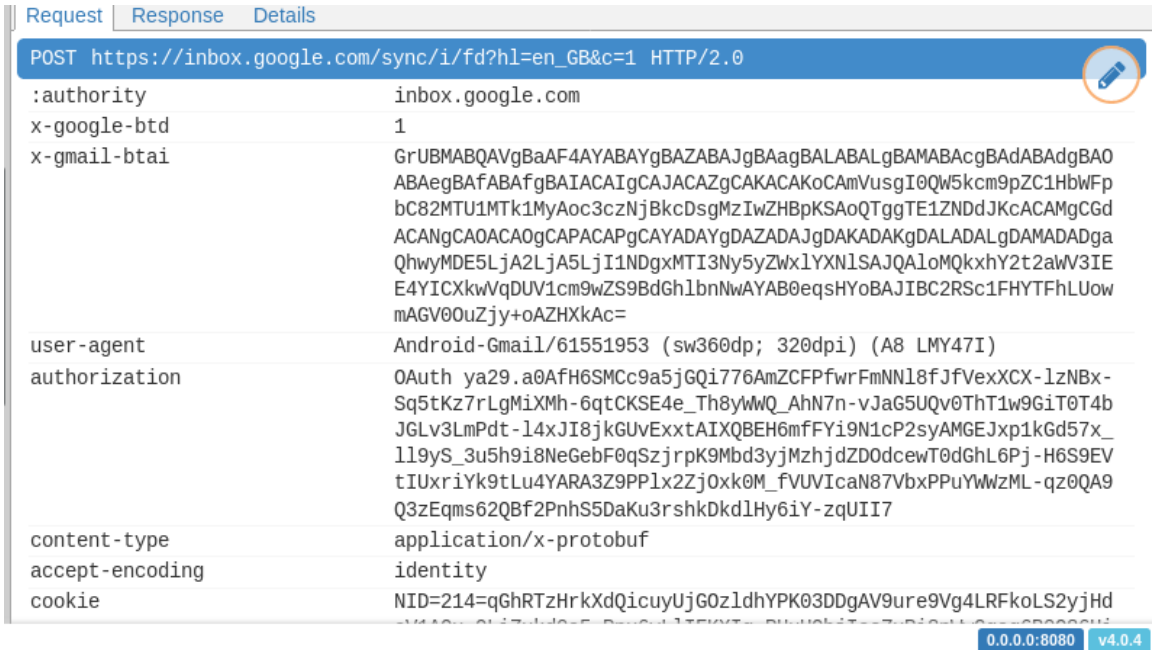
ΕΙΚΟΝΑ 26:ΑΠΟΚΑΛΥΨΗ ΤΟΠΟΘΕΣΙΑΣ ΣΤΗ GOOGLE

Κάνει αιτήματα προς τη google, της μορφής όπως φαίνεται στην Εικόνα 27, αποκαλύπτοντας το μοντέλο της συσκευής και το baseband version της συσκευής.



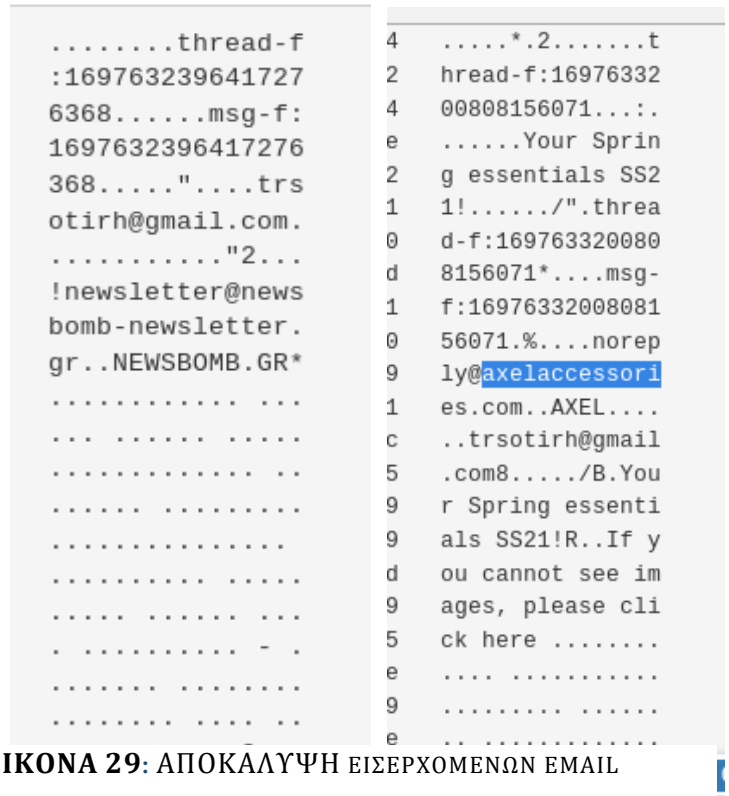
ΕΙΚΟΝΑ 27:ΑΠΟΚΑΛΥΨΗ ΤΟΥ ΜΟΝΤΕΛΟΥ ΤΗΣ ΣΥΣΚΕΥΗΣ ΣΤΟ PLAY.GOOGLEAPIS

Κάνει αιτήματα προς το inbox της Google που είναι της μορφής όπως φαίνεται στην εικόνα 28.



ΕΙΚΟΝΑ 28:Αιτήματα προς το inbox.google

Αποθηκεύει cookie (NID=214….) αποκαλύπτοντας το email μας όπως φαίνεται παρακάτω, το android id , ακόμα και δύο email που έχουμε στα εισερχόμενα μας, το newsletter@newsbomb-newsletter.gr και το noreply@axelaccessories.com, όπως φαίνεται στην Εικόνα 29.



ΕΙΚΟΝΑ 29: ΑΠΟΚΑΛΥΨΗ ΕΙΣΕΡΧΟΜΕΝΩΝ EMAIL

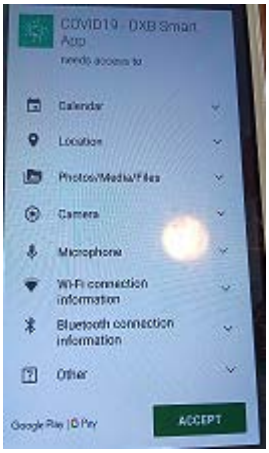
Κάνει αιτήματα της μορφής όπως φαίνονται στην εικόνα 30, αποκαλύπτοντας το androdID, το email και την έκδοση των google_play_services.

ΕΙΚΟΝΑ 30:ΕΥΡΗΜΑΤΑ ΑΠΟ ΤΟ ANDROID.GOOGLEAPIS.COM

Συχνά η εφαρμογή συνδέεται με το pl.gov.mc.protegosafe για να λάβει πληροφορίες σχετικά με τα κλειδιά που έχουν δημοσιευθεί. Εάν σταματήσουμε τη χρήση της και την «αφήσουμε» στο παρασκήνιο, τότε συνεχίζει να συνδέεται με τη Firebase και λιγότερο συχνά με τη pl.gov.mc.protegosafe. Όταν μάλιστα πατήσαμε και στην επιλογή «click gov. pl.gr», η σελίδα μας αποθήκευσε ένα cookie και εμφανίστηκαν άλλα δύο αιτήματα προς τη Google, «update.googleapis.com»,αποκαλύπτονταςτο«userid="{68ebda95a044dbe433ecd4f9fba47430}» και το «appid": "gcmjkmgdlgnkkcocmoeiminaijmmjnii"».

6.2.2 Covid19-DXB Smart App

Η δεύτερη εφαρμογή που θα ελέγξουμε είναι η Covid19-DXB Smart App η οποία είναι εφαρμογή του Ντουμπάι για την αντιμετώπιση της πανδημίας, δηλαδή σε μία χώρα εκτός ΕΕ. Χρησιμοποιούμε το blackview A8 με έκδοση λογισμικού android 5. Η εφαρμογή στηρίζεται στο κεντρικοποιημένο σύστημα και για αυτό ζητά από τον χρήστη να κάνει εγγραφή και του στέλνει OTP (βλ Εικόνα 32) για να πιστοποιήσει την αυθεντικότητά του. Η εγγραφή περιλαμβάνει όνομα, επίθετο, αριθμό διαβατηρίου και τηλεφώνου.

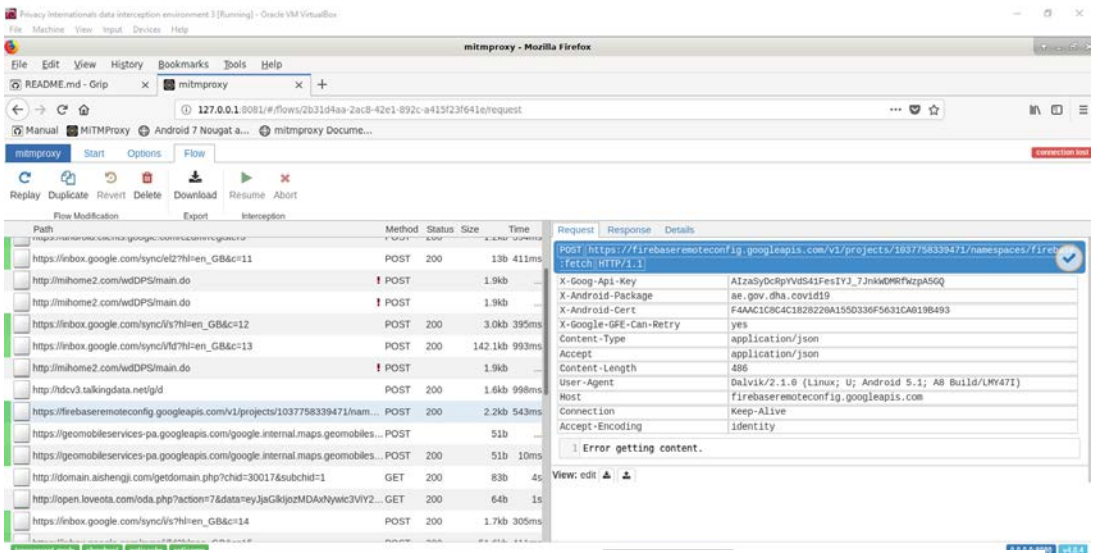


ΕΙΚΌΝΑ 31: ΠΡΟΣΒΑΣΕΙΣ ΕΦΑΡΜΟΓΗΣ

ΕΙΚΟΝΑ 32: OTP

Είναι μια πολύ εύκολη εφαρμογή η οποία παρέχει συμβουλές στους χρήστες για τι πρέπει να κάνουν εάν έχουν νοσήσει, τι πρέπει να κάνουν ώστε να προστατευθούν από τον κίνδυνο μόλυνσής τους και να ζητήσουν βοήθεια εάν δεν αισθάνονται καλά είτε από ασθενοφόρο είτε από την αστυνομία είτε από τον επίσημο υγειονομικό φορέα του Ντουμπάι. Ενημερώνει τον χρήστη για τα τελευταία νέα όσον αφορά τον ιό και τα εμβόλια που γίνονται στον κόσμο καθώς και τις τελευταίες μελέτες για τα εμβόλια ανά τον κόσμο. Αυτό που σαφώς προβληματίζει είναι οι προσβάσεις που ζητάει για να λειτουργήσει η εφαρμογή, το ημερολόγιο, την κάμερα, το μικρόφωνο, την τοποθεσία και τα αρχεία που βρίσκονται μέσα στην κινητή εφαρμογή (βλ Εικόνα 31).

Αφού εγκαταστήσουμε την εφαρμογή, την «ανοίγουμε», διαλέγουμε τη γλώσσα (Αγγλικά), τρέχουμε το mitmproxy_start.sh και κάνουμε διάφορες δοκιμές για 320 δευτερόλεπτα. Τα αποτελέσματα του εικονικού περιβάλλοντος είναι αυτά που φαίνονται στην Εικόνα 33.



ΕΙΚΟΝΑ 33: ΑΠΟΤΕΛΕΣΜΑΤΑ COVID19-DXB SMART APP ΜΕ ΤΟ PI_MANINTHEMIDDLE

Βλέπουμε ότι η εφαρμογή, η οποία είναι επίσημη εφαρμογή της κυβέρνησης του Ντουμπάι, συνδέεται με τον διακομιστή ΄ae.gov.dha.covid19’ για να «κατεβάσει» τα αναγνωριστικά που έχουν δημοσιοποιηθεί. Μετά την εγκατάσταση, συνδέεται με την firebase πλατφόρμα της google και αποκαλύπτει το "fid": "ebs5NukFQ-GWqklIRt5jVm" στην Google ,το οποίο είναι το αναγνωριστικό της firebase και στην ουσία αποκαλύπτει την τωρινή κατάστασή της. Αποστέλλει στη Google το αναγνωριστικό της εφαρμογής(appId) και την έκδοση του SDK(sdkVersion), (βλ. Εικόνα 34) και εκείνη «απαντάει» με 2 token(authToken,refreshToken).


```
{
    "appId": "1:1037758339471:android:de233c4299ca54f810d3fa",
    "authVersion": "FIS_v2",
    "fid": "ebs5NukFQ-GWqklIRt5jVm",
    "sdkVersion": "a:16.3.0"
}
```


ΕΙΚΟΝΑ 34:ΤΟ FID ΤΟΥ FIREBASE

Κάνει αιτήματα προς τη «firebaseremoteconfig.googleapis.com» και αποκαλύπτει την έκδοση του android της συσκευής που χρησιμοποιούμε, την ημερομηνία και τη χρονική στιγμή που εγκαθιδρύθηκε η σύνδεση, την ζώνη ώρας που έχουμε βάλει στη συσκευή, τη γλώσσα που χρησιμοποιούμε καθώς επίσης και το αναγνωριστικό της τωρινής κατάστασης της εφαρμογής (appIntsnaceID=”ebs5NukFQ….). Βρήκαμε και το όνομα του “domain” που είναι το «domain.aishengji.com/getdomain».

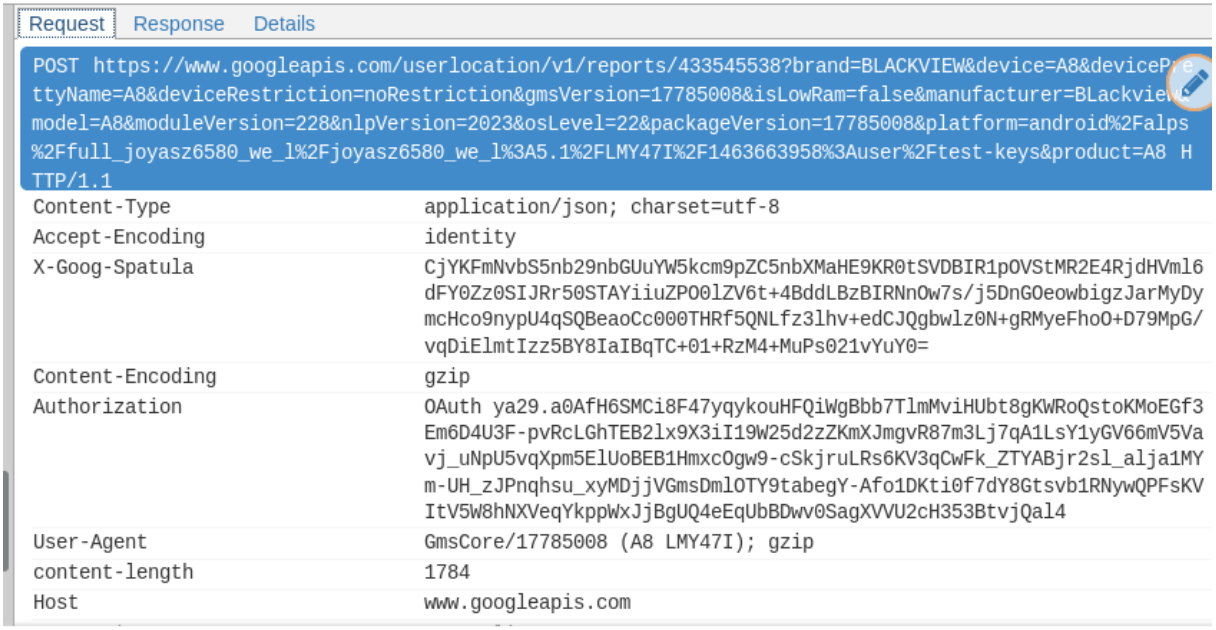
Όσον αφορά τα αιτήματα που κάνει η εφαρμογή προς τη Google πέρα από τη firebase, είναι της μορφής όπως φαίνονται παρακάτω στην εικόνα 35 και στην οποία αποκαλύπτει το μοντέλο της συσκευής, το σειριακό της αριθμό (SERIAL 123456789ABCDEF), τον κατασκευαστή, το σειριακό αριθμό του HARDWARE, το FINGERPRINT.


```
POST https://www.googleapis.com/androidantiabuse/v1/x/create?alt=PROTO&key=AIzaSyBofcZsgLSS7BOnBjZPE
4rYwzOIz-lTI HTTP/1.1
```

Content-Type	application/x-protobuf
User-Agent	DroidGuard/17785008
Content-Length	808
Host	www.googleapis.com
Connection	Keep-Alive
Accept-Encoding	identity

Εικόνα 35:Αιτήματα προς το googleapis.com.

Άλλα αιτήματα προς την Google στην οποία και αποκαλύπτει το ιστορικό του χρήστη, τι έψαξε στο διαδίκτυο ή τα βίντεο που έχει παρακολουθήσει είναι όπως φαίνονται στην εικόνα 36.



Εικονα 36:Αιτηματα προς το googleapis.com/location

Άλλα αιτήματα προς τη Google, είναι της μορφής όπως φαίνεται στην εικόνα 37 και αποκαλύπτει το email μας, 'trsotirh@gmail.com' λόγω του viber που έχουμε στη συσκευή.

Εικόνα 37:ΑΙΤΗΜΑΤΑ ΠΡΟΣ ΤΟ viber-ΑΠΟΚΑΛΥΨΗ ΤΟΥ email

Παρατηρήσαμε ότι όταν πατήσαμε στην επιλογή κοινή χρήση μέσω του viber «share the app via viber» , αποκάλυψε το IMEI της συσκευής, τον τηλεφωνικό μας αριθμό, το αναγνωριστικό του χρήστη, τον κωδικό της χώρας που είμαστε καθώς και την MAC διεύθυνσή μας.

ΕΙΚΟΝΑ 38: ΑΠΟΚΑΛΥΨΗ ΤΟΥ IMEI ΑΠΟ ΤΟ VIBER

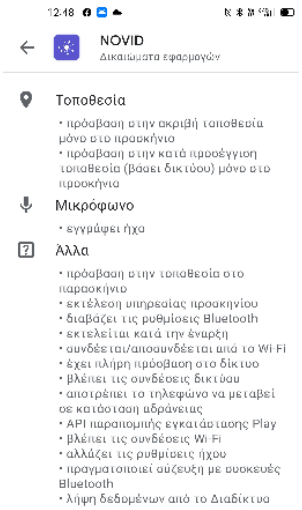
Περαιτέρω, συνδέεται με τη 'SafetyNet' και αποκαλύπτεται το αναγνωριστικό της εφαρμογής (app Instance Id[5]). Μόλις πατήσαμε στην καρτέλα «Privacy Policy», μας ανακατεύθυνε στη σελίδα «www.dha.gov.ae» η οποία μας πρόσθεσε και ένα cookie(dha.gov.ae=1441202442.20480.0000;). Όταν πατήσαμε στην επιλογή «πάρε βοήθεια» (Get Help), άνοιξε το GPS ,προφανώς για να βρουν την τοποθεσία μας εάν χρειαζόμασταν όντως βοήθεια, κάνοντας αιτήματα προς το "geomobileservices-pa.googleapis.com" που είναι μια νόμιμη υπηρεσία (API) που παρέχεται από την Google maps.

Από τα ανωτέρω καθίσταται σαφές ότι η εν λόγω εφαρμογή εάν λειτουργούσε σε χώρες της ΕΕ, θα ήταν μη συμμορφούμενη με τις προϋποθέσεις νόμιμης επεξεργασίας προσωπικών δεδομένων.

[5] Το Instance ID παρέχει ένα μοναδικό αναγνωριστικό για κάθε παρουσία της εφαρμογής και έναν μηχανισμό ελέγχου ταυτότητας και εξουσιοδότησης ενεργειών, όπως η αποστολή μηνυμάτων μέσω Firebase Cloud Messaging.Ο χρήστης για να το διαγράψει, εκτελεί "Εκκαθάριση δεδομένων" στην εφαρμογή.

6.2.3 NOVID

Η τρίτη εφαρμογή ιχνηλάτησης επαφών που θα ελέγξουμε είναι η NOVID η οποία έχει δημιουργηθεί στην Αμερική και η οποία στηρίζεται στο αποκεντρωμένο σύστημα. Δεν δίνει το δικαίωμα στον χρήστη να αυτοανακηρυχθεί θετικά διαγνωσμένος, παρά μόνο όταν τοποθετήσει τον κωδικό του τεστ που έχει κάνει από πιστοποιημένο διαγνωστικό κέντρο.

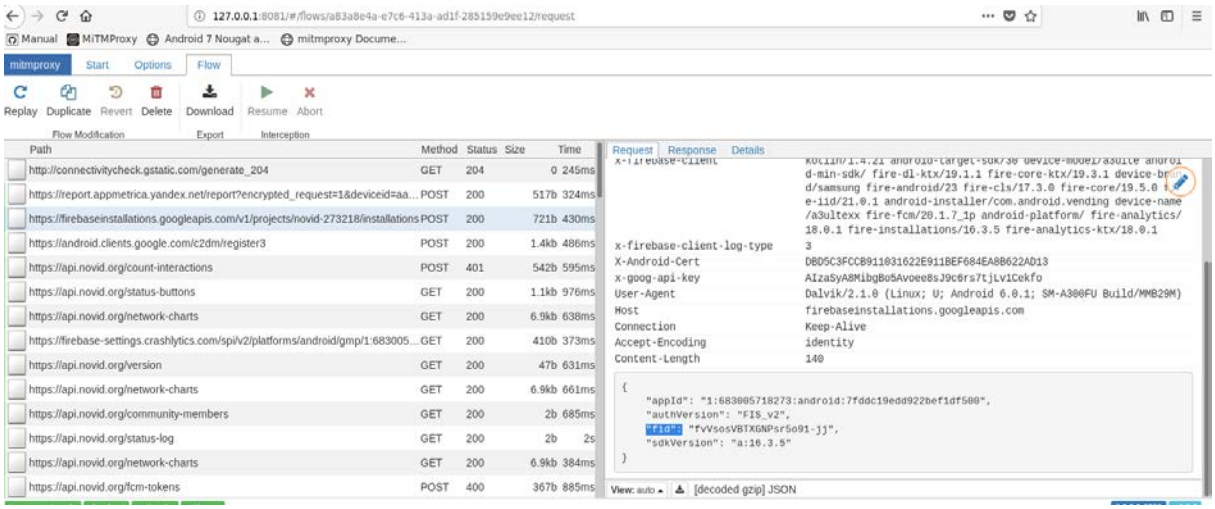


ΕΙΚΟΝΑ 39: ΠΡΟΣΒΑΣΕΙΣ ΕΦΑΡΜΟΓΗΣ NOVID

Βέβαια εντύπωση μας κάνουν οι αποδοχές στις άδειες που ζητάει η χρήση της εφαρμογής, όπως για παράδειγμα την εγγραφή στο ηχείο όπως φαίνεται στην Εικόνα 39 και η πρόσβαση στην τοποθεσία. Αυτές τις πληροφορίες τις βρήκαμε στις πληροφορίες της εφαρμογής στο Google Play Store.

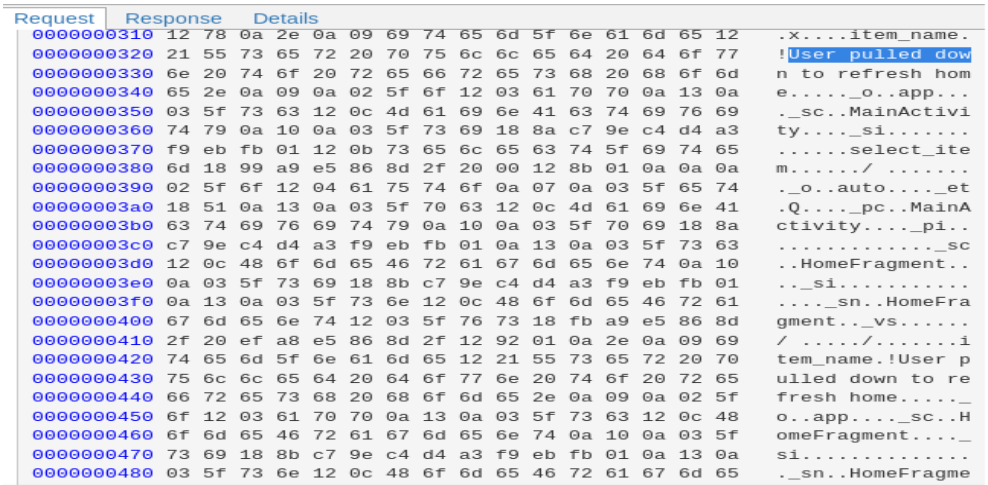
Η εφαρμογή, ενημερώνει το χρήστη αν έχει έρθει κοντά με άτομα που έχουν εκτεθεί, το πόσο «κοντά» το διευκρινίζει μάλιστα λέγοντάς τους ότι θα πρέπει να έχουν έρθει σε απόσταση κάτω των 3^{ων} μέτρων και για πάνω από 15 λεπτά. Βέβαια όταν απενεργοποιήσαμε το Bluetooth δεν μας επισήμανε να το ξανανοίξουμε και αυτό διότι χρησιμοποιεί έναν συνδυασμό από Bluetooth, WiFi και υπερήχους, λαμβάνοντας και στέλνοντας ανώνυμα αναγνωριστικά. Τονίζει μάλιστα στις πληροφορίες της, ότι δεν χρησιμοποιεί το GPS διότι δεν είναι αξιόπιστο για ιχνηλάτηση επαφών.

Από τα αποτελέσματα παρατηρούμε ότι η εφαρμογή κατά την εγκατάστασή της, συνδέεται με την Firebase όπου και το "fid":fvVsosVBTXGNPsr5o91-jj (το αναγνωριστικό της Firebase) όπως φαίνεται στην Εικόνα 40.



ΕΙΚΟΝΑ 40: ΑΠΟΤΕΛΕΣΜΑΤΑ PI_MANINTHEMIDDLE ΤΗΣ ΕΦΑΡΜΟΓΗΣ NOVID

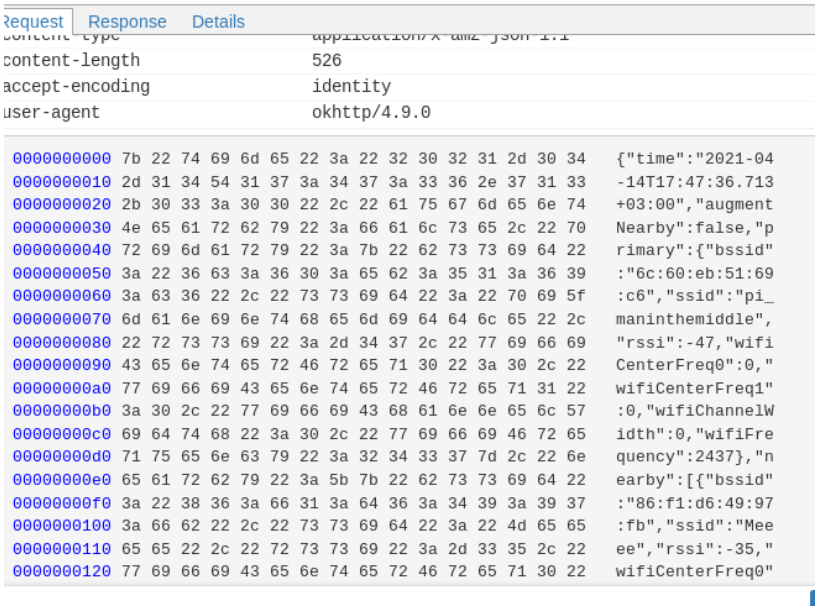
Αποκαλύπτεται το μοντέλο και η έκδοση του android μας. Φαίνεται ότι ο διακομιστής και επομένως η Αρχή που είναι υπεύθυνη για την εφαρμογή είναι η «api.novid.org». Συνδέεται με την Firebase Analytics «firebase-settings.crashlytics.com» ώστε να καταγράψει δεδομένα καθώς ο χρήστης αλληλεπιδρά με την εφαρμογή. Αυτό που μας εξέπληξε είναι το "user pulled down to refresh home" όπως φαίνεται στην εικόνα 41, διότι όντως καθώς επεξεργαστήκαμε την εφαρμογή, ανανεώσαμε τη σελίδα για να «φορτώσουν» επιπλέον δεδομένα. Αποκαλύπτει το αναγνωριστικό του χρήστη «userId":"e18b9 e80-b4bc-4457-b6 12-bd7dd3869bf9" (Google Advertising ID). Η εφαρμογή κάνει συνεχώς connectivitycheck.gstatic.com ώστε να ελέγξει τη σύνδεση με το διαδίκτυο.



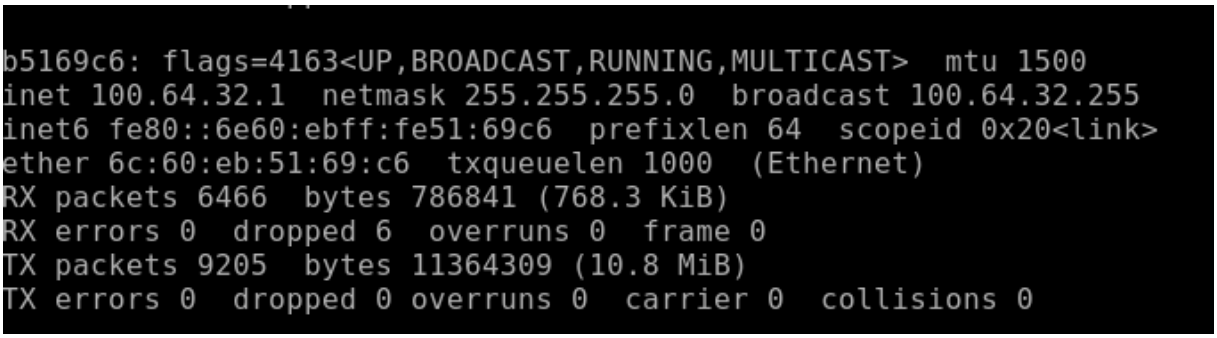
ΕΙΚΟΝΑ 41: ΑΠΟΤΕΛΕΣΜΑΤΑ PI_MANINTHEMIDDLE

Στη συνέχεια παρατηρούμε το «novid-user-id» το οποίο αποτελεί το αναγνωριστικό εφαρμογής του χρήστη, την έκδοση της εφαρμογής «android;4.7.0-rc.1».

Στη συνέχεια, αποκαλύπτει το όνομα του WiFi που χρησιμοποιούμε (βλ Εικόνα 42) καθώς και τη MAC διεύθυνσή μας (φαίνεται ξεκάθαρα ποια είναι στην εικόνα 43).



Εικονα 42:ΑΠΟΚΑΛΥΨΗ ΤΟΥ WIFI



Εικονα 43:MAC ΔΙΕΥΘΥΝΣΗ ΤΗΣ ΣΥΣΚΕΥΗΣ ΜΑΣ

Εντύπωση προκαλεί η παρακάτω Εικόνα 44:

```
0000000160 69 46 72 65 71 75 65 6e 63 79 22 3a 32 34 33 37   iFrequency":2437
0000000170 7d 2c 7b 22 62 73 73 69 64 22 3a 22 38 63 3a 36   },{"bssid":"8c:6
0000000180 38 3a 63 38 3a 63 63 3a 32 36 3a 36 63 22 2c 22   8:c8:cc:26:6c","
0000000190 73 73 69 64 22 3a 22 4d 41 52 49 4c 45 4e 41 2d   ssid":"MARILENA-
00000001a0 58 52 49 53 54 4f 53 22 2c 22 72 73 73 69 22 3a   XRISTOS","rssi":
00000001b0 2d 38 34 2c 22 77 69 66 69 43 65 6e 74 65 72 46   -84,"wifiCenterF
00000001c0 72 65 71 30 22 3a 32 34 35 37 2c 22 77 69 66 69   req0":2457,"wifi
00000001d0 43 65 6e 74 65 72 46 72 65 71 31 22 3a 32 34 35   CenterFreq1":245
00000001e0 37 2c 22 77 69 66 69 43 68 61 6e 6e 65 6c 57 69   7,"wifiChannelWi
00000001f0 64 74 68 22 3a 31 2c 22 77 69 66 69 46 72 65 71   dth":1,"wifiFreq
0000000200 75 65 6e 63 79 22 3a 32 34 33 37 7d 5d 7d         uency":2437}]}
```

ΕΙΚΟΝΑ 44: ΑΠΟΚΑΛΥΨΗ ΤΟΥ WIFI ΔΙΠΛΑΝΩΝ ΣΠΙΤΙΩΝ

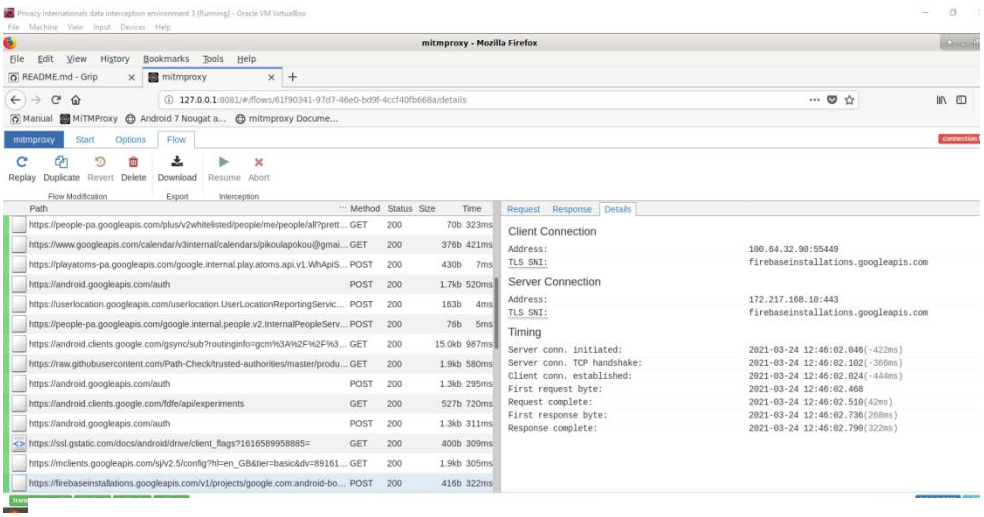
Μέσω της εφαρμογής αποκαλύπτονται τα ονόματα των WiFi διπλανών σπιτιών «https://api.novid.org/wifi-bssid-nearby». Περαιτέρω, χρησιμοποιεί τη «nexus-websocket-a.intercom.io» στην οποία επίσης αποκαλύπτεται το αναγνωριστικό του χρήστη intercomId : «6b5ab076-4b8e-42 d1-98ed-e46446bb ad6b». Η εφαρμογή έχει την επιλογή, αν θέλουμε φυσικά, να προσθέσουμε ένα ιστορικό με τα άτομα που έχουμε βρεθεί , το όνομα και το email τους. Εμείς για παράδειγμα προσθέσαμε μια εικονική «επαφή» και παρατηρήσαμε ότι η εφαρμογή τη «μοιράστηκε» με τον διακομιστή. Φυσικά μαζί του «μοιράζεται» και την ημερομηνία και ώρα εγκαθίδρυσης της σύνδεσης. Τέλος, προσπάθησε να συνδεθεί με το Facebook μόνο όταν πατήσαμε πάνω στην επιλογή «share this app to Facebook».

6.2.4 SafePlaces

Η επόμενη εφαρμογή που θα ελέγξουμε είναι η SafePlaces, η οποία ονομαζόταν παλιά Safe Paths, και είναι μια εφαρμογή για Covid-19 του MIT και είναι βασισμένη σε δεδομένα τοποθεσίας και όχι στο Bluetooth.

ΕΙΚΌΝΑ 45: ΠΡΟΣΒΑΣΕΙΣ ΤΗΣ SAFEPLACES

Στην Εικόνα 45 φαίνονται οι προσβάσεις που «ζητάει» η εφαρμογή. Την άδεια στην τοποθεσία τη ζητάει διότι η εφαρμογή αποθηκεύει τις τοποθεσίες που έχει επισκεφθεί ο χρήστης για δέκα τέσσερις ημέρες. «Εντύπωση» δίνει η άδεια που ζητάει στον αποθηκευτικό χώρο της κινητής συσκευής να τροποποιεί ή να διαγράφει το περιεχόμενο του κοινόχρηστου αποθηκευτικού χώρου, κάτι το οποίο δεν θα πρέπει να «κάνει» μια εφαρμογή ιχνηλάτησης. Εάν κάποιος διαγνωστεί θετικός τότε με τη συγκατάθεσή του μοιράζεται το ημερολόγιο των τοποθεσιών που έχει επισκεφθεί ώστε να ενημερωθούν και άλλοι χρήστες ότι έχουν βρεθεί σε μέρος όπου κάποιος συμπολίτης τους έχει διαγνωστεί θετικός με τεστ από πιστοποιημένο διαγνωστικό κέντρο. Η εφαρμογή δοκιμάστηκε από εμάς στη χώρα μας αλλά δουλεύει σωστά στην Αμερική και αυτό διότι έχει μια επιλογή από τοποθεσίες που μπορεί ο χρήστης να επιλέξει και οι οποίες βρίσκονται στην Αμερική. Όπως ήταν αναμενόμενο η εφαρμογή συνδέεται με το Firebase της google (από την αποδοχή της υπηρεσίας ειδοποιήσεων έκθεσης) όπως φαίνεται στην Εικόνα 46 και καταγράφει την τοποθεσία του χρήστη «userlocation.googleapis.com» και το ιστορικό του «history.google.com» .



ΕΙΚΟΝΑ 46: ΑΠΟΤΕΛΕΣΜΑΤΑ SAFE PLACES

Αποκαλύπτεται το email μας, το androidID και η γλώσσα όπως φαίνεται στην Εικόνα 47.

```
0000000000 61 6e 64 72 6f 69 64 49 64 3d 33 33 35 36 35 61   androidId=33565a
0000000010 36 32 30 37 31 30 35 34 36 37 26 6c 61 6e 67 3d   6207105467&lang=
0000000020 65 6e 5f 47 42 26 67 6f 6f 67 6c 65 5f 70 6c 61   en_GB&google_pla
0000000030 79 5f 73 65 72 76 69 63 65 73 5f 76 65 72 73 69   y_services_versi
0000000040 6f 6e 3d 31 37 37 38 35 30 30 38 26 73 64 6b 5f   on=17785008&sdk_
0000000050 76 65 72 73 69 6f 6e 3d 32 32 26 64 65 76 69 63   version=22&devic
0000000060 65 5f 63 6f 75 6e 74 72 79 3d 67 72 26 63 6c 69   e_country=gr&cli
0000000070 65 6e 74 5f 73 69 67 3d 33 38 39 31 38 61 34 35   ent_sig=38918a45
0000000080 33 64 30 37 31 39 39 33 35 34 66 38 62 31 39 61   3d07199354f8b19a
0000000090 66 30 35 65 63 36 35 36 32 63 65 64 35 37 38 38   f05ec6562ced5788
00000000a0 26 63 61 6c 6c 65 72 53 69 67 3d 33 38 39 31 38   &callerSig=38918
00000000b0 61 34 35 33 64 30 37 31 39 39 33 35 34 66 38 62   a453d07199354f8b
00000000c0 31 39 61 66 30 35 65 63 36 35 36 32 63 65 64 35   19af05ec6562ced5
00000000d0 37 38 38 26 45 6d 61 69 6c 3d 74 72 73 6f 74 69   788&Email=trsoti
00000000e0 72 68 25 34 30 67 6d 61 69 6c 2e 63 6f 6d 26 68   rh%40gmail.com&h
00000000f0 61 73 5f 70 65 72 6d 69 73 73 69 6f 6e 3d 31 26   as_permission=1&
0000000100 73 65 72 76 69 63 65 3d 6f 61 75 74 68 32 25 33   service=oauth2%3
0000000110 41 68 74 74 70 73 25 33 41 25 32 46 25 32 46 77   Ahttps%3A%2F%2Fw
0000000120 77 77 2e 67 6f 6f 67 6c 65 61 70 69 73 2e 63 6f   ww.googleapis.co
0000000130 6d 25 32 46 61 75 74 68 25 32 46 74 61 63 68 79   m%2Fauth%2Ftachy
0000000140 6f 6e 26 61 70 70 3d 63 6f 6d 2e 67 6f 6f 67 6c   on&app=com.googl
0000000150 65 2e 61 6e 64 72 6f 69 64 2e 67 6d 73 26 63 68   e.android.gms&ch
0000000160 65 63 6b 5f 65 6d 61 69 6c 3d 31 26 74 6f 6b 65   eck_email=1&toke
```

ΕΙΚΟΝΑ 47: ΑΠΟΚΑΛΥΨΗ ANDROIDID, EMAIL ΚΑΙ ΤΗΣ ΓΛΩΣΣΑΣ ΤΗΣ ΣΥΣΚΕΥΗΣ

Κάνει αιτήματα προς τη Google, αποκαλύπτοντας την έκδοση του android της συσκευής, το μοντέλο, το αναγνωριστικό του android (androidID) και το email μας. Τα αιτήματα είναι της μορφής όπως φαίνονται στην Εικόνα 48:

Request | Response | Details

`POST https://android.googleapis.com/auth HTTP/1.1`

device	33565a6207105467
app	com.google.android.gms
Accept-Encoding	identity
User-Agent	GoogleAuth/1.4 (A8 LMY47I); gzip
content-length	1318
content-type	application/x-www-form-urlencoded
Host	android.googleapis.com
Connection	Keep-Alive

ΕΙΚΟΝΑ 48: ΑΙΤΗΜΑΤΑ ΤΗΣ ΕΦΑΡΜΟΓΗΣ SAFE PLACES ΠΡΟΣ ΤΟ ANDROID.GOOGLEAPIS.COM

Στη συνέχεια αποκαλύπτονται το ημερολόγιο, η ζώνη ώρας, και οι επαφές μας. Φαίνεται ότι η υπεύθυνη αρχή για αυτή την εφαρμογή είναι η «cdn.safeplaces.cloud». Η εφαρμογή μας ζητάει να επιλέξουμε το τμήμα υγείας (που μας εξυπηρετεί), το οποίο φαίνεται και στο εργαλείο μας (κάτι που είναι φυσικό μιας και αποτελεί πληροφορία που μεταδίδεται στον διακομιστή). Διαλέξαμε για τους ερευνητικούς μας σκοπούς, το "Southern Methodist University" το οποίο φαίνεται και στην εικόνα 49 μαζί με τις συντεταγμένες που βρίσκεται το πανεπιστήμιο.

```
authorities:
  - name: Southern Methodist University
    bounds:
      ne:
        latitude: 32.84519188749405
        longitude: -96.77456683457996
      sw:
        latitude: 32.840775057560634
        longitude: -96.7949301654212
    org_id: cbc199b8-f9f1-47f1-a4bc-cd86cb629131
    public_api: https://ingest.smu.backend.safeplaces.cloud
    cursor_url: https://cdn.safeplaces.cloud/004smu/cursor.json
  - name: Teton County, WY Health Department
    bounds:
      ne:
        latitude: 44.182231277676266
        longitude: -109.1243588328588
      sw:
        latitude: 43.06836443689707
```

ΕΙΚΟΝΑ 49: ΣΥΝΤΕΤΑΓΜΕΝΕΣ ΤΟΥ SOUTHERN METHODIST UNIVERSITY

Κάνει αιτήματα προς το «history.google.com» και "history_recording_enabled:true", αποθηκεύοντας το ιστορικό του χρήστη (άλλωστε η εφαρμογή αποθηκεύει τα μέρη που επισκέφθηκε ο χρήστης).

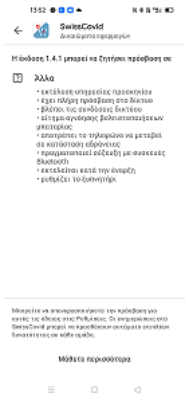
Αυτό που μας έκανε εντύπωση είναι ότι όταν έκανε αιτήματα προς το «inbox.google.com», εμφανίστηκαν και διευθύνσεις που υπάρχουν στα εισερχόμενα email μας (info@websuplies, myshoe@myshoe.gr), όπως φαίνεται και παρακάτω στην Εικόνα 50. Μάλιστα τη δεύτερη φορά που δοκιμάσαμε την εφαρμογή, αποκάλυψε και άλλες διευθύνσεις email που βρίσκονται στα εισερχόμενά μας.

Άρα και σε αυτήν την περίπτωση, η εφαρμογή δεν θα πληρούσε τις προϋποθέσεις νόμιμης επεξεργασίας αν ήταν σε λειτουργία στην Ε.Ε.

ΕΙΚΟΝΑ 50: ΑΠΟΚΑΛΥΨΗ ΕΙΣΕΡΧΟΜΕΝΩΝ EMAILS

6.2.5 SwissCovid

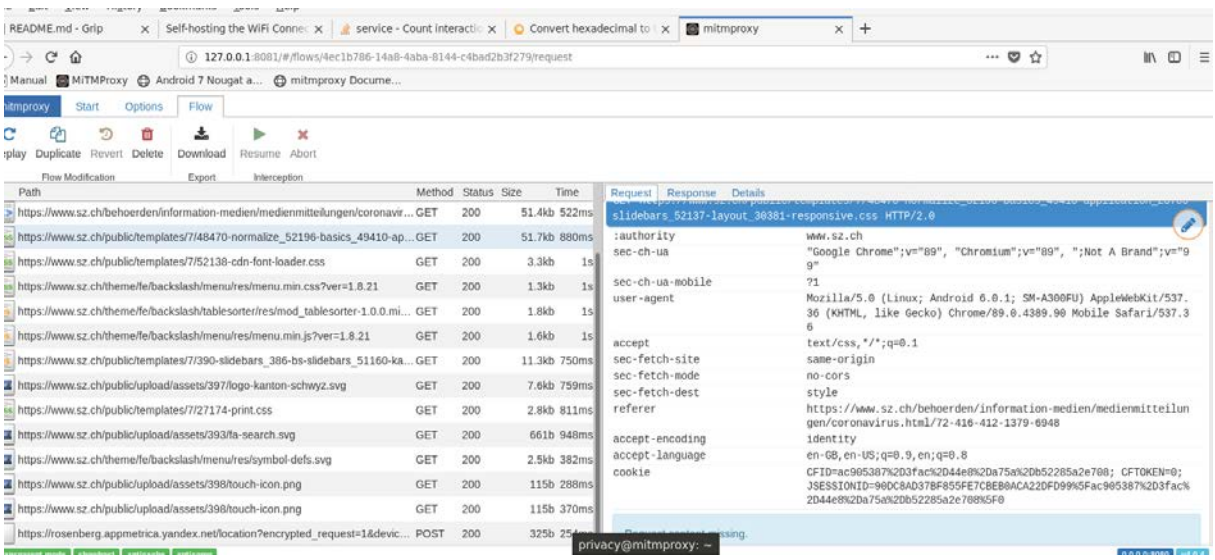
Η επόμενη εφαρμογή που θα ελέγξουμε είναι η SwissCovid που είναι εφαρμογή της Ελβετίας και η οποία στηρίζεται στο DP3T αποκεντρωμένο σύστημα οπότε και δεν χρειάζεται εγγραφή του χρήστη. Δημιουργήθηκε στις 25 Μαΐου του 2020. Δεν ζητάει περαιτέρω πρόσβαση στην κινητή συσκευή του χρήστη όπως φαίνεται και παρακάτω στην Εικόνα 51.



ΕΙΚΟΝΑ 51: ΠΡΟΣΒΑΣΕΙΣ ΤΗΣ ΕΦΑΡΜΟΓΗΣ SWISSCOVID

Ένα από τα μειονεκτήματα της εφαρμογής είναι ότι περιορίζεται στην Ελβετία οπότε και δεν στηρίζει τη διαλειτουργικότητα ανάμεσα στις χώρες της ΕΕ. Στηρίζεται στο Bluetooth και μόνο και τονίζει ρητά και ξεκάθαρα ότι ο υπεύθυνος επεξεργασίας της εφαρμογής είναι το ομοσπονδιακό γραφείο δημόσιας υγείας της που βρίσκεται στην Ελβετία. Ζητάει να ενεργοποιηθούν οι ειδοποιήσεις έκθεσης και το Bluetooth. Δεν αφήνει ένα χρήστη να αυτοανακηρυχθεί θετικός παρά μόνο εάν τοποθετήσει κωδικό από τεστ πιστοποιημένου διαγνωστικού κέντρου. Τα αναγνωριστικά που αποθηκεύονται τοπικά στην κινητή συσκευή διαγράφονται μετά από 14 μέρες. Όπως φαίνεται και παρακάτω στην Εικόνα 52 δεν μπορέσαμε να βρούμε αλληλεπιδράσεις που έχει η εφαρμογή με άλλες εφαρμογές διότι, όπως μας ενημέρωσε «δεν μπορεί να λειτουργήσει σωστά εκτός εάν απενεργοποιήσουμε τον proxy που χρησιμοποιούμε και αυτός είναι και ο λόγος που συνεχώς κάνει αιτήματα της μορφής «connectivitycheck.gstatic.com».

Μόνο όταν επιλέξαμε την επιλογή «πρόσθετες πληροφορίες» και «που μπορώ να εξεταστώ», ανοίγοντάς μας επιπλέον ιστοσελίδα στο Google Chrome, της Ελβετίας με πληροφορίες για το που θα εξεταστούμε εάν παρουσιάζουμε συμπτώματα, βρήκαμε ότι αποκαλύπτεται το μοντέλο της συσκευής και η έκδοση του λογισμικού που έχουμε. Σύμφωνα με το [5], μετά την εγκατάσταση, η εφαρμογή συνδέεται συνεχώς με τον διακομιστή για να «κατεβάσει» τα αναγνωριστικά από χρήστες που νόσησαν. Τα «αιτήματα» αυτά, δεν περιλαμβάνουν ”cookies”. Σε κάθε περίπτωση, η εν λόγω εφαρμογή δεν φαίνεται να εγείρει ζητήματα ιδιωτικότητας.



ΕΙΚΟΝΑ 52: ΑΠΟΤΕΛΕΣΜΑΤΑ ΤΗΣ ΕΦΑΡΜΟΓΗΣ SWISSCOVID ΜΕ ΤΟ PI_MANINTHEMIDDLE

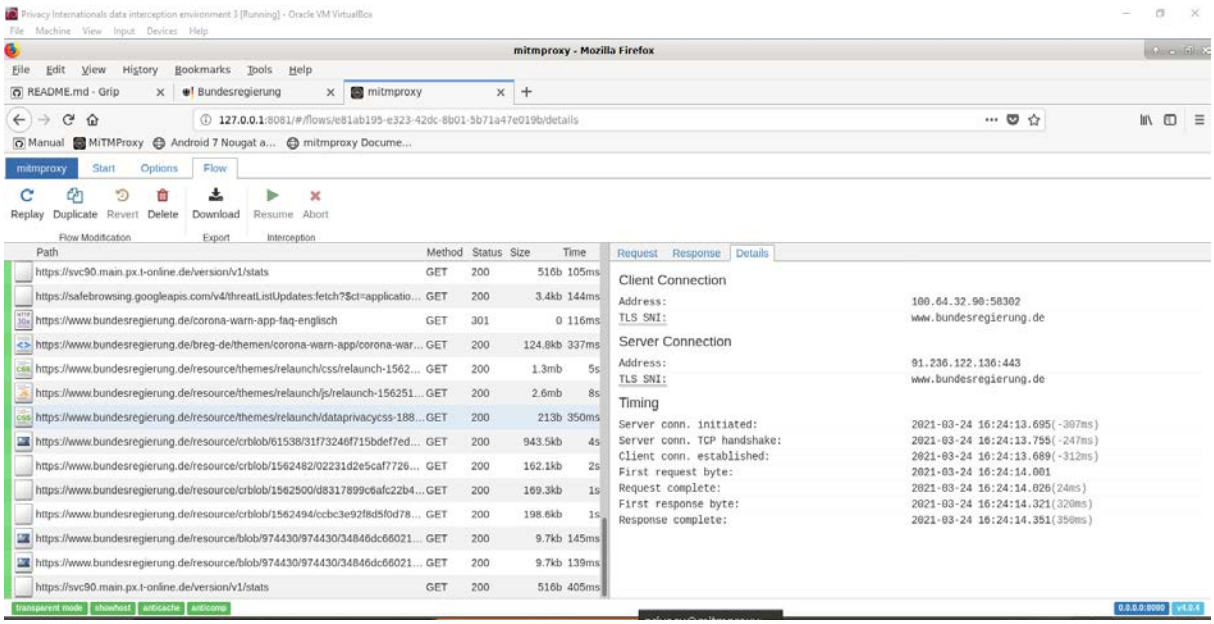
6.2.6 Immuni

Η επόμενη εφαρμογή ιχνηλάτησης είναι η Immuni που είναι η επίσημη εφαρμογή της Ιταλίας και αναπτύχθηκε από τον έκτακτο Επίτροπο για την πανδημία Covid-19 (Extraordinary Commissioner for the COVID-19 Emergency) σε συνεργασία με το Υπουργείο Υγείας και το Υπουργείο Τεχνολογικής Καινοτομίας και Ψηφιοποίησης. Στηρίζεται στο αποκεντρωμένο σύστημα και στην υπηρεσία ειδοποίησης έκθεσης της Google/Apple μέσω BLE. Με το που εγκαθίσταται η εφαρμογή, δεν ζητάει περαιτέρω πρόσβαση στα συστήματα της κινητής συσκευής. Αρχικά ενημερώνει το χρήστη ότι τα δεδομένα του αποθηκεύονται τοπικά στη συσκευή του και ότι η σύνδεση με τον διακομιστή είναι κρυπτογραφημένη. Ακολούθως, τονίζει ότι η εφαρμογή ενημερώνει ότι το υπουργείο Υγείας της χώρας έχει αναλάβει τον έλεγχο του διακομιστή. Ζητάει στη συνέχεια τον τόπο που μένει ο χρήστης και αν έχει ειδοποιηθεί ότι είναι σε μεγάλο κίνδυνο έκθεσης στον ιό. Δεν ζητάει εγγραφή, ούτε τηλέφωνο. Δεν καταγράφει την τοποθεσία μέσω GPS. Τέλος η εφαρμογή συνδέεται μία φορά την ημέρα με τον διακομιστή στην Ιταλία για να κατεβάσει τα αναγνωριστικά των θετικά διαγνωσμένων χρηστών και να τα ελέγξει με αυτά που είναι αποθηκευμένα τοπικά στη συσκευή ώστε να τον ειδοποιήσει ότι βρίσκεται σε κίνδυνο. Ο χρήστης μπορεί να ανεβάσει με τη συγκατάθεσή του στον διακομιστή ότι έχει διαγνωστεί θετικά αφού έχει κάνει τεστ σε πιστοποιημένο διαγνωστικό κέντρο. Τέλος η ιταλική κυβέρνηση τονίζει ξεκάθαρα ότι τα δεδομένα διατηρούνται στον διακομιστή για 14 ημέρες και σε κάθε περίπτωση το αργότερο μέχρι τις 31 Δεκεμβρίου του 2021. Ένα μειονέκτημα που παρατηρήσαμε είναι ότι ενώ φαίνεται ότι στηρίζει τη διαλειτουργικότητα εάν πάμε να αλλάξουμε χώρα σταματάει να λειτουργεί και «κρασάρει». Δυστυχώς μέσω του εργαλείου δεν βρήκαμε πολλά, διότι η εφαρμογή δεν συμβάδιζε με τον mitmproxy «client may not trust the proxy's certificate for get.imuni.gov.it». Στην αρχή, η εφαρμογή συνδέεται με τον διακομιστή για να «κατεβάσει» τα αναγνωριστικά από χρήστες που νόσησαν. Τα «αιτήματα» αυτά, δεν περιλαμβάνουν "cookies" ή άλλα αναγνωριστικά που να αφορούν την εφαρμογή. Καθώς λειτουργεί στο παρασκήνιο, συνδέεται τακτικά με τον διακομιστή για να κατεβάσει αναγνωριστικά και δημόσια κλειδιά από χρήστες που νόσησαν. Το μόνο που βρήκαμε είναι ότι η εφαρμογή αποκάλυψε το μοντέλο της κινητής συσκευής (το οποίο παρόλο που πράγματι αφορά επεξεργασία προσωπικών δεδομένων, δεν εγείρει σοβαρά ζητήματα ιδιωτικότητας).

6.2.7 Corona-Warn-App

Η επόμενη εφαρμογή είναι η Corona-Warn-App της Γερμανίας η οποία δημιουργήθηκε από το Ινστιτούτο Robert Koch(RKI) υπό την ιδιότητα του ως κεντρικού ομοσπονδιακού ιδρύματος για

τη δημόσια υγεία εκ μέρους της γερμανικής κυβέρνησης. Χρησιμοποιεί BLE και τις υπηρεσίες ειδοποιήσεων έκθεσης της Google/Apple. Δεν χρειάζεται εγγραφή. Υποστηρίζει τη διαλειτουργικότητα αλλά όχι για όλες τις χώρες της ΕΕ, παρά μόνο για την Αυστρία, Βέλγιο, Κροατία, Κύπρο, Δανία, Ιταλία, Λετονία ,Σλοβενία, Νορβηγία, Πολωνία, Σουηδία, Ιρλανδία, Τσεχία και φυσικά στη Γερμανία. Δεν ζητάει περαιτέρω προσβάσεις με την εγκατάσταση, αλλά αν παρατηρήσουμε την περιγραφή της στο Google play Store, βλέπουμε ότι έχει πρόσβαση στη φωτογραφική μηχανή της συσκευής. Τέλος δίνει στον χρήστη τη δυνατότητα να δημιουργήσει ένα ημερολόγιο με τα μέρη και τα άτομα που συναντήθηκε και να βάλει τον αριθμό και το ηλεκτρονικό του ταχυδρομείο.



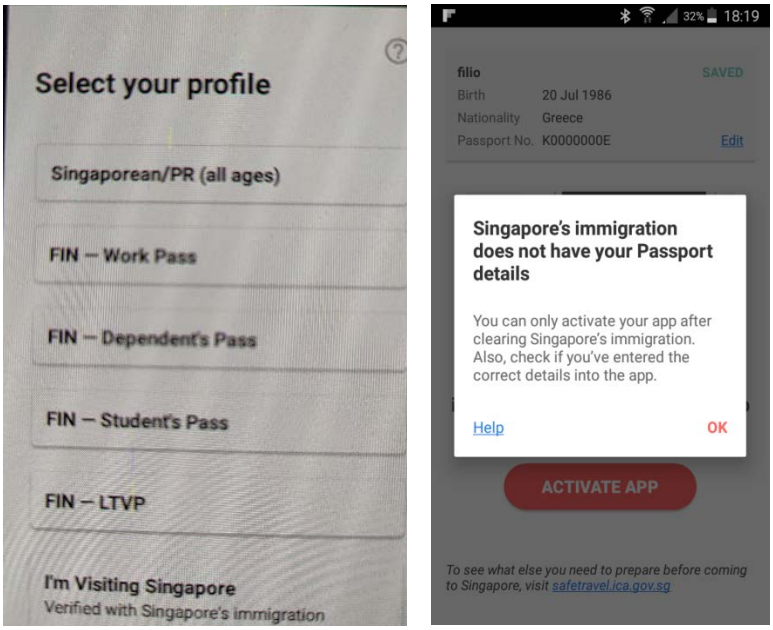
ΕΙΚΟΝΑ 53:ΑΠΟΤΕΛΕΣΜΑΤΑ CORONA-WARN-APP

Όπως βλέπουμε στην Εικόνα 53, συνδέεται με την επίσημη ιστοσελίδα της Γερμανίας. Αποκαλύπτει το αναγνωριστικό της εφαρμογής, το μοντέλο της συσκευής, την έκδοση του λογισμικού της. Βλέπουμε ότι η κατάστασή μας (status OK) που φαίνεται στη συσκευή, φαίνεται και στο εργαλείο και αυτό διότι η εφαρμογή κάνει «ερωτήματα» προς τον διακομιστή για αναγνωριστικά θετικά διαγνωσμένων χρηστών, τα οποία ελέγχει για να αξιολογήσει την κατάσταση του χρήστη της (εδώ είναι εντάξει «OK»). Η διεύθυνση του διακομιστή είναι 87.140.208.250:443. Δεν βρέθηκαν «cookies» στα «αιτήματα» προς τον διακομιστή, ούτε άλλα αναγνωριστικά τα οποία να συνδέονται με την τωρινή κατάσταση της εφαρμογής. Καθώς η εφαρμογή «έτρεχε» στο παρασκήνιο, συνδεόταν τακτικά με τον διακομιστή για να κατεβάσει αναγνωριστικά χρηστών που έχουν νοσήσει και άλλες ρυθμίσεις οι οποίες όμως δεν περιείχαν

αναγνωριστικά για την κατάσταση της εφαρμογής. Σε κάθε περίπτωση η εφαρμογή δεν φαίνεται να εγείρει σοβαρά ζητήματα ιδιωτικότητας.

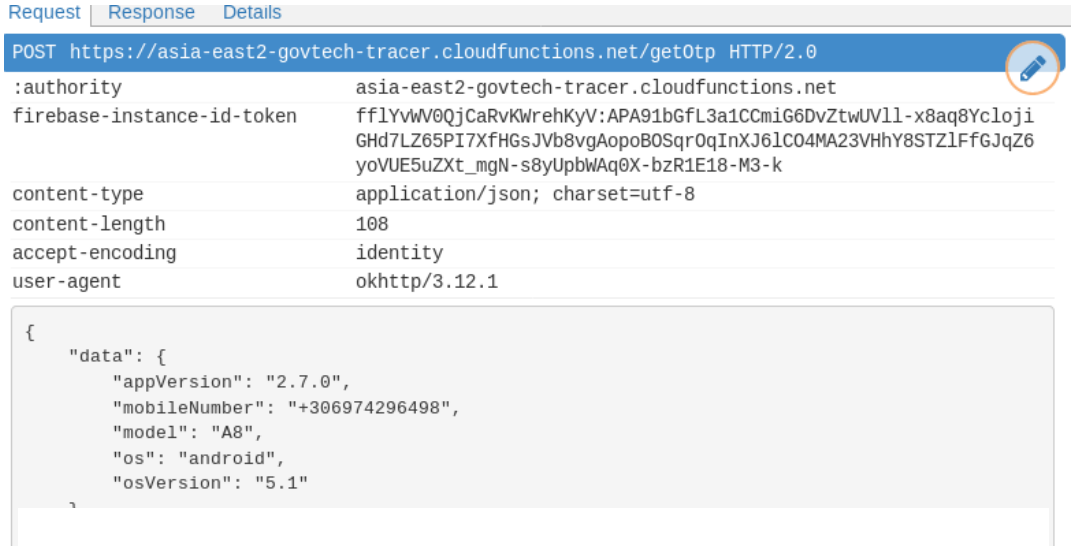
6.2.8 Trace Together

Η εφαρμογή Trace Together της Σιγκαπούρης, πρόκειται για μία από τις πιο γνωστές εφαρμογές του κόσμου και στηρίζεται στο πρωτόκολλο bluetrace. Κατά την εκκίνηση της εφαρμογής, μας ζητήθηκε OTP και στη συνέχεια να διαλέξουμε ένα από τα παρακάτω προφίλ , αλλά δυστυχώς δεν μπορούσαμε να προχωρήσουμε στην εγκατάστασή της (βλ. Εικόνα 54) διότι ελέγχει, βάσει των στοιχείων ταυτοποίησης που εισάγουμε, αν είμαστε πράγματι τοπικοί κάτοικοι (ο έλεγχος γίνεται με την ταυτότητά μας) ή επισκέπτες (ο έλεγχος γίνεται με το διαβατήριο).



ΕΙΚΟΝΑ 54: ΤΑΥΤΟΠΟΙΗΣΗ ΤΟΥ ΧΡΗΣΤΗ ΜΕ ΤΗΝ ΕΦΑΡΜΟΓΗ

Αυτό που κάναμε είναι να ελέγξουμε την εφαρμογή μέχρι σε αυτό το σημείο οπότε και βρήκαμε τα παρακάτω αποτελέσματα που φαίνονται στην εικόνα 55.



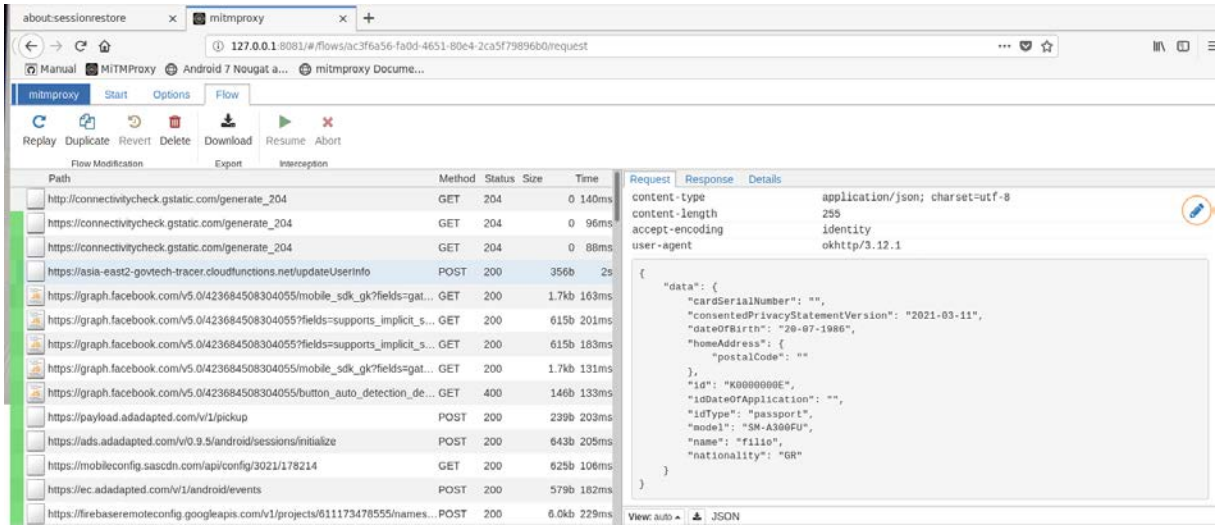
Εικονα 55: ΜΕΤΑΔΟΣΗ ΤΗΛΕΦΩΝΟΥ ΤΟΥ ΧΡΗΣΤΗ ΣΤΟΝ ΔΙΑΚΟΜΙΣΤΗ ΚΑΙ ΑΠΟΣΤΟΛΗ OTP

Από ότι φαίνεται στην Εικόνα, η εφαρμογή κατά την εκκίνηση δεν «κατεβάζει» εφήμερα αναγνωριστικά από την Firebase, παρά μόνο στέλνει στον διακομιστή τα στοιχεία της σύνδεσής μας για την αποστολή του OTP, τον αριθμό που δηλώσαμε, το μοντέλο της συσκευής μας και την έκδοση του λογισμικού που χρησιμοποιούμε (android).

Στη συνέχεια, επικοινωνεί με τον διακομιστή «asia-east2-govtech-tracer.cloudfunctions.net» και του στέλνει την έκδοση της εφαρμογής (appVersion=2.7.0) καθώς και το OTP ώστε να γίνει η πιστοποίηση της αυθεντικότητας του χρήστη (βλ Εικόνα 56).

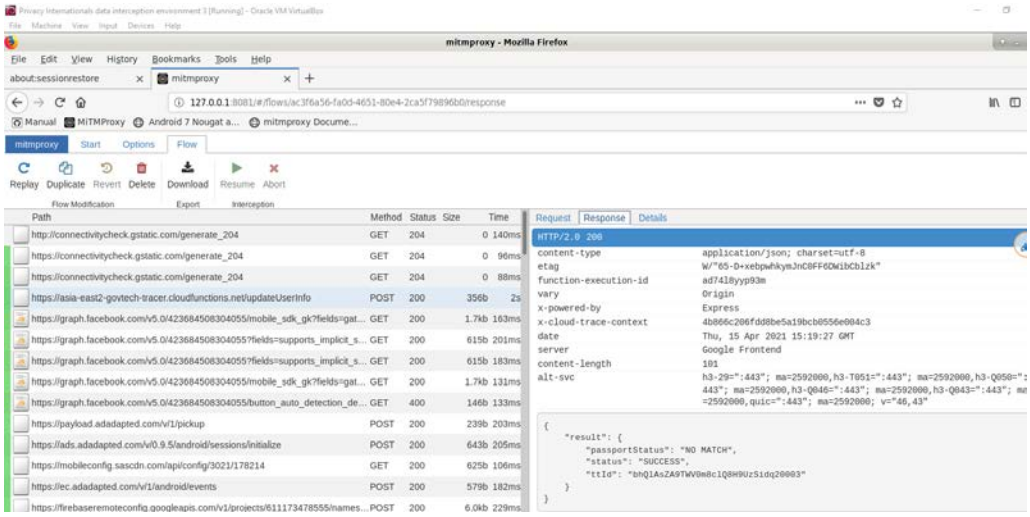
ΕΙΚΟΝΑ 56:ΔΗΜΙΟΥΡΓΙΑ ΧΡΗΣΤΗ ΣΤΟΝ ΔΙΑΚΟΜΙΣΤΗ ΤΗΣ ΕΦΑΡΜΟΓΗΣ

Στη συνέχεια (βλ. Εικόνα 57) αποκαλύπτεται στον διακομιστή το όνομα «filio» που δηλώσαμε κατά την εγγραφή, τον τύπο πιστοποίησης της αυθεντικότητάς μας που διαλέξαμε, δηλαδή το διαβατήριο «passport», την εθνικότητα που βάλαμε «GR», την ημερομηνία γέννησής μας «20-07-1986» και την αποδοχή της άδειας ιδιωτικότητας της εφαρμογής με ημερομηνία έκδοσής της «2021-03-11». Η εφαρμογή κάνει συνεχώς αιτήματα σύνδεσης προς τον διακομιστή της.



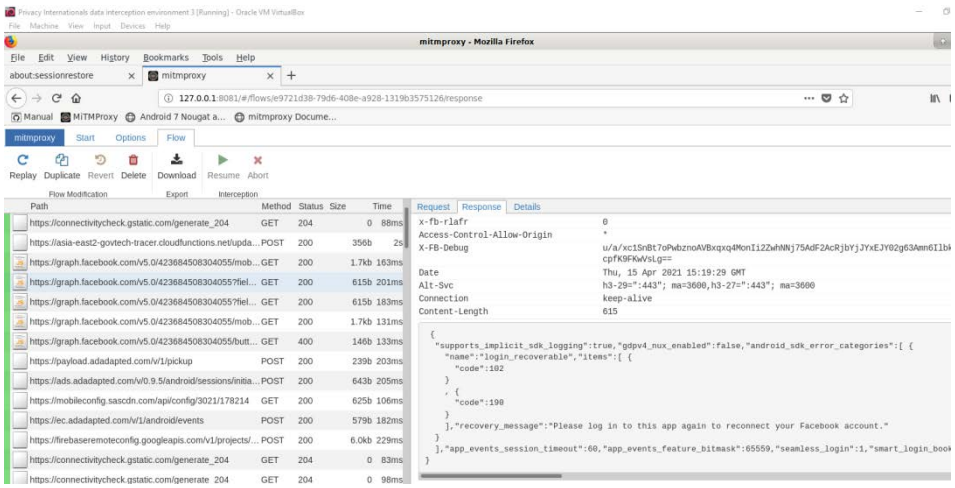
ΕΙΚΟΝΑ 57: ΑΠΟΣΤΟΛΗ ΣΤΟΙΧΕΙΩΝ ΤΟΥ ΧΡΗΣΤΗ ΣΤΟΝ ΔΙΑΚΟΜΙΣΤΗ

Στη συνέχεια, επειδή το διαβατήριο δεν ήταν σωστό (μας επισημαίνει ότι κανένας τουρίστας με αυτό το διαβατήριο δεν έχει εισέλθει στην Σιγκαπούρη), είναι κάτι το οποίο φαίνεται κ στην παρακάτω εικόνα 58 με το «passport no match». Αν και προφανώς ο ΓΚΠΔ, δεν έχει εφαρμογή στην περίπτωση αυτή, φαίνεται ότι η εφαρμογή κάνει ελέγχους με άλλες βάσεις δεδομένων της χώρας για έλεγχο ταυτοποίησης χρήστη-κάτι το οποίο καθιστά σαφές ότι αν ήταν σε λειτουργία στην Ευρώπη δεν θα ήταν συμβατή με το ευρωπαϊκό νομικό πλαίσιο για την προστασία δεδομένων. Παρά την ανωτέρω διαπίστωση βέβαια, συνεχίσαμε την ανάλυσή μας μέχρι το σημείο που ήταν εφικτό, όπως περιγράφεται στη συνέχεια.



ΕΙΚΟΝΑ 58: ΑΠΟΤΥΧΙΑ ΠΙΣΤΟΠΟΙΗΣΗΣ ΤΟΥ ΧΡΗΣΤΗ

Στη συνέχεια αποκαλύπτει το σειριακό αριθμό της συσκευής (SERIAL), το δαχτυλικό αποτύπωμα (FINGERPRINT). Παρατηρούμε ακόμα ότι συνδέεται με το «FACEBOOK GRAPH» όπως φαίνεται παρακάτω (βλ. Εικόνα 59) και συνδέεται με το «adsFacebookMediaViewEnabled:true» για διαφημιστικούς λόγους.



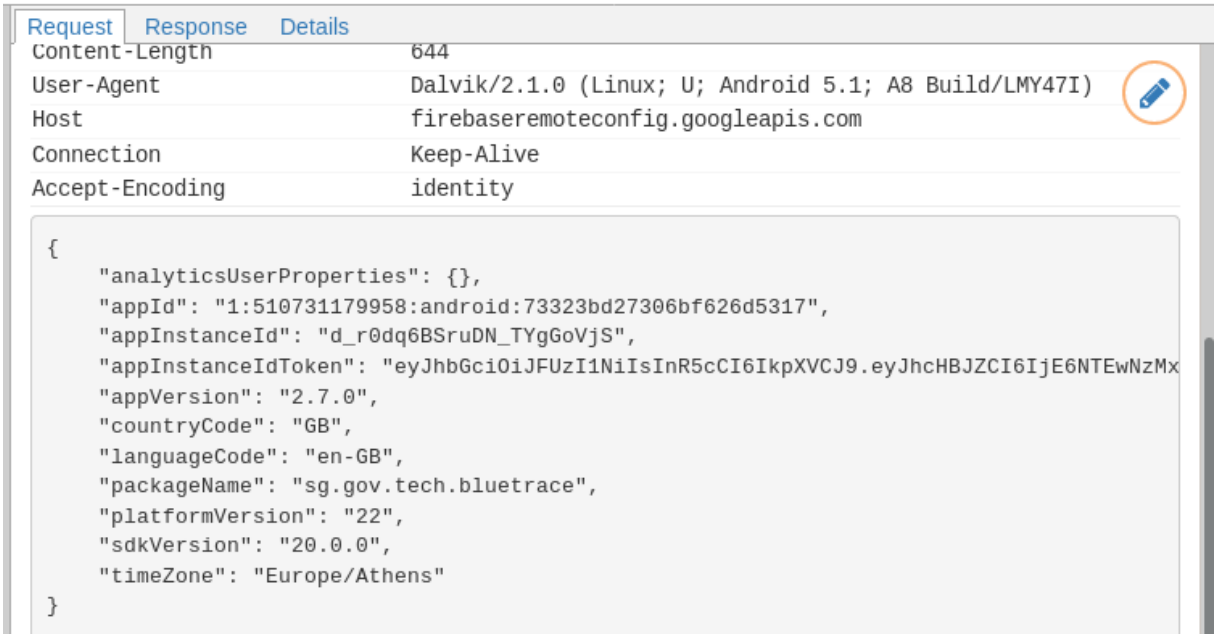
ΕΙΚΟΝΑ 59: ΣΥΝΔΕΣΗ ΕΦΑΡΜΟΓΗΣ ΜΕ ΤΟ FACEBOOK GRAPH

Συνεχίζουμε τη μελέτη μας, χρησιμοποιώντας και την άλλη κινητή μας συσκευή (Samsung A3, android6 και κάρτα sim «Vodafone»). Βλέπουμε λοιπόν ότι στην Εικόνα 60, αποκαλύπτει και πάλι το μοντέλο της συσκευής, το λογισμικό της, το αναγνωριστικό της εφαρμογής «app_id": "NTKXMZFJZTA2NMZJ», το αναγνωριστικό του χρήση, την ώρα ζώνης της συσκευής, τον πάροχο του δικτύου «vodafone GR» και συνδέεται με διακομιστή διαφημίσεων «Smartadserver» και

«adCallBaseURL: https://www14.smartadserver.com» το οποίο χρησιμοποιείται για την ανάλυση διαφημίσεων και χρηστών.

ΕΙΚΟΝΑ 60: ΑΠΟΚΑΛΥΨΗ ΔΕΔΟΜΕΝΩΝ ΤΟΥ ΧΡΗΣΤΗ

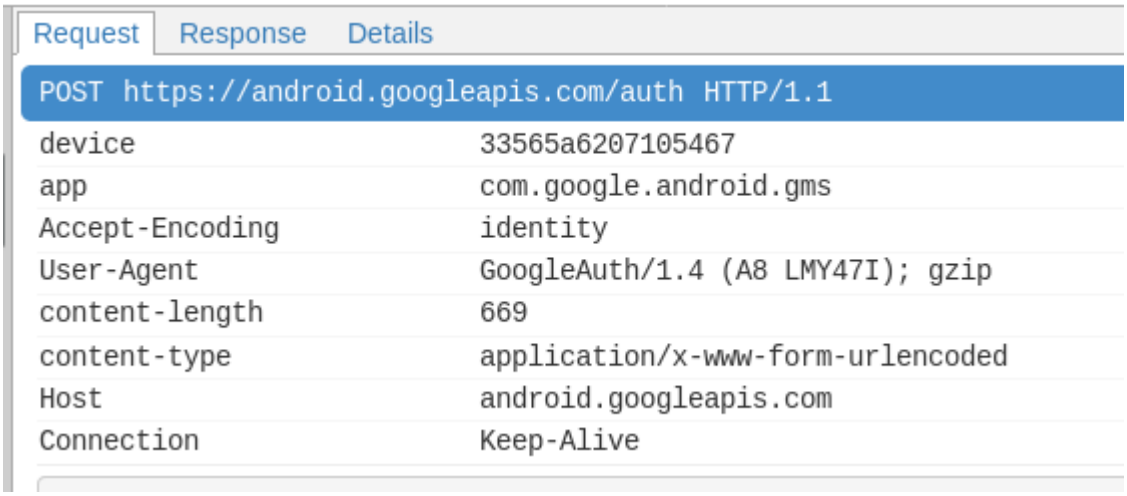
Καθώς προχωράμε με την εγκατάσταση της εφαρμογής, παρατηρούμε ότι συνδέεται με την Firebase firebaseinstallations.googleapis.com με «fid: d_r0dq6BSruDN_TYgGoVjS» και με τη «firebaseremoteconfig.googleapis.com» και προφανώς χρησιμοποιεί τη Firebase απομακρυσμένη (Remote) διαμόρφωση (configuration), όπως φαίνεται στην εικόνα 61:



ΕΙΚΟΝΑ 61: FIREBASE REMOTE CONFIG.

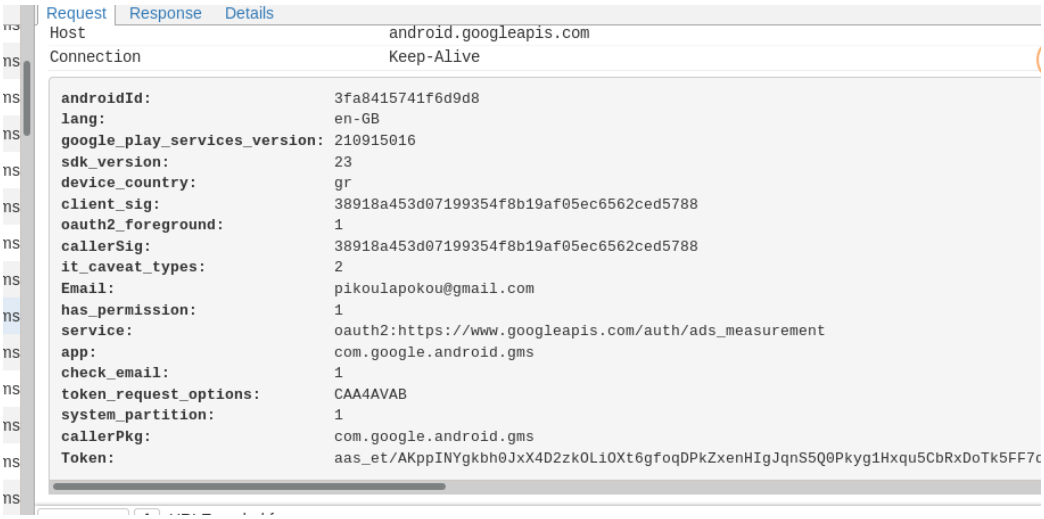
Φαίνεται από την εικόνα ότι αποκαλύπτει το αναγνωριστικό της εφαρμογής, τη γλώσσα και τη ζώνη ώρας της συσκευής. Ακόμα, κάνει αιτήματα και προς τη firebase.crashlytics.com η οποία συλλέγει στατιστικά στοιχεία για το χρήστη και τη συμπεριφορά του.

Όσον αφορά το GAEN, η Trace Together κάνει συνεχώς αιτήματα προς το «android.googleapis.com», της μορφής όπως φαίνεται παρακάτω στην Εικόνα 62:



ΕΙΚΟΝΑ 62: ΑΙΤΗΜΑΤΑ ΤΗΣ ΕΦΑΡΜΟΓΗΣ ΠΡΟΣ ΤΟ ANDROID.GOOGLEAPIS.COM

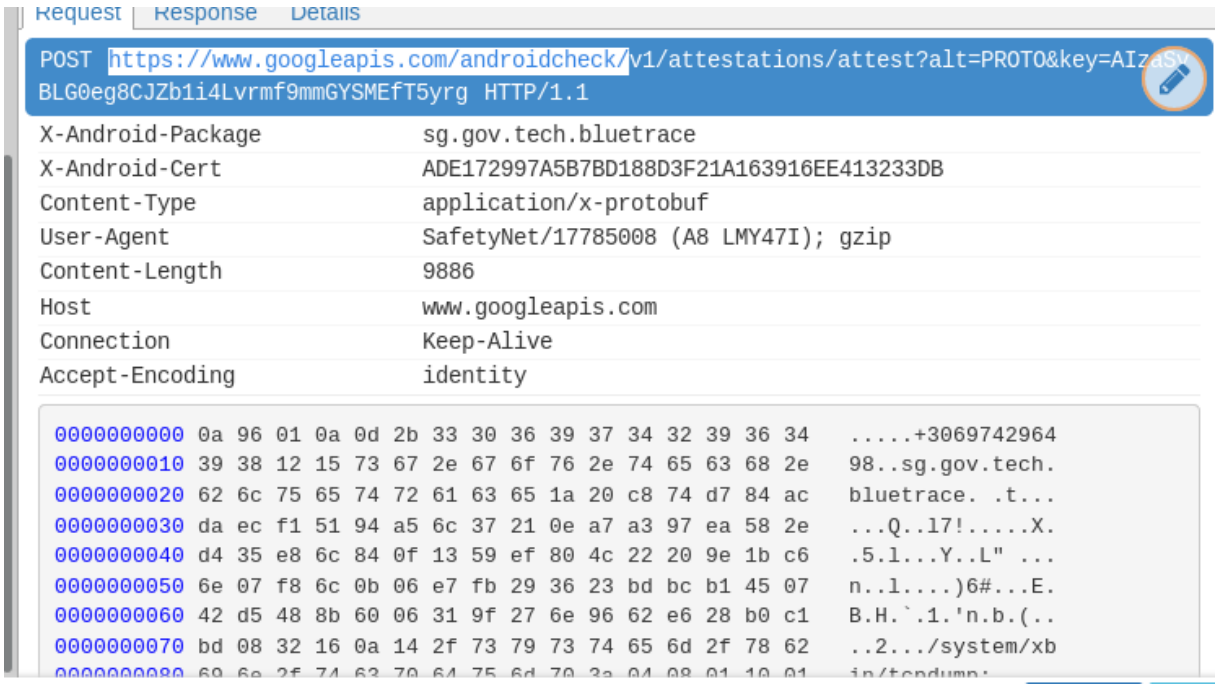
Με το συγκεκριμένο αίτημα όπως φαίνεται και στην εικόνα 63 αποκαλύπτει στη Google το email μας (είναι διαφορετικό με πριν μιας και όπως προαναφέραμε χρησιμοποιήσαμε τη δεύτερη συσκευή μας).



ΕΙΚΟΝΑ 63:ΑΠΟΚΑΛΥΨΗ ΤΟΥ EMAIL ΣΤΗ GOOGLE

Παρατηρούμε επίσης ότι αυτό το αίτημα σύνδεσης χρησιμοποιεί και άλλες υπηρεσίες της Google, όπως τις «googleapis.com/auth/webhistory», «googleapis.com/auth/plus.media.upload», «googleapis.com/auth/plus.profiles.read» και «googleapis.com/auth/plus.peopleapi.readwrite».

Η εφαρμογή κάνει αιτήματα προς «semanticlocation-pa.googleapis.com» αποκαλύπτοντας την τοποθεσία του χρήστη, κάνει αιτήματα προς το «com.google.android.youtube» και προς το www.google.com/complete/search το οποίο συνοδεύεται από cookie τα οποία "cookies" στέλνουν το μόνιμα αναγνωριστικά (persistent identifier) τα οποία μπορούν να συνδεθούν μεταξύ τους και σε συγκεκριμένο χρήστη. Στη συνέχεια, αποκαλύπτει το μοντέλο και το build number "MMB29M.A300FUXXU1CRF1" της συσκευής. Κάνει αιτήματα προς το «android.googleapis.com/androidcheck», τα οποία είναι της μορφής όπως φαίνεται στην εικόνα 64 και παρατηρούμε ότι αποκαλύπτει το τηλέφωνο που δώσαμε στην αρχή για την ταυτοποίησή μας:



ΕΙΚΟΝΑ 64: ΑΠΟΚΑΛΥΨΗ ΤΗΛΕΦΩΝΟΥ ΣΤΗ GOOGLEAPIS.COM

Όσο η εφαρμογή βρίσκεται στο παρασκήνιο, κάνει αιτήματα προς το «decide.mixpanel.com», μια υπηρεσία τρίτου μέρους που αναλαμβάνει στατιστικά εφαρμογών και κινητών συσκευών καθώς και την «app-measurement.com», την οποία χρησιμοποιεί η Google Analytics για να

αναφέρει αναλυτικά το τι κάνει ο χρήστης. (Μάλιστα από τη στιγμή που έχουμε «κολλήσει» στο διαβατήριο, όντως το αναφέρει με το «BoardProfilePassport»).

Η ανάλυσή μας, σταμάτησε εδώ γιατί δεν μπορούσαμε να προχωρήσουμε στην εγκατάσταση της εφαρμογής.

Βέβαια, αξίζει να σημειωθεί ότι έχει γίνει πολλή έρευνα για τη συγκεκριμένη εφαρμογή και μάλιστα είναι από τις πιο γνωστές και πολυσυζητημένες εφαρμογές στον κόσμο και μάλιστα όπως προαναφέραμε εκτός ΕΕ. Στο [11]οι συγγραφείς τονίζουν ότι σε σύγκριση με άλλες λύσεις, ένα πλεονέκτημα του TraceTogether είναι ότι παρέχει στο Υπουργείο Υγείας τη δυνατότητα σχεδίασης του γραφήματος μετάδοσης του COVID-19 στο πληθυσμό που έχει εγκαταστήσει την εφαρμογή. Μπορεί να γίνει εύκολα με βάση το γεγονός ότι τα προσωρινά αναγνωριστικά συνδέονται με τους αριθμούς τηλεφώνου, οι οποίοι μπορούν να βοηθήσουν το Υπουργείο Υγείας να προσδιορίζει τους χρήστες. Αυτό το πλεονέκτημα είναι απόρροια του κόστους της χρησιμότητας εις βάρος του απορρήτου των χρηστών.

6.2.9 Συγκεντρωτικά συγκριτικά αποτελέσματα

Συνολικά τα ευρήματα μας συνοψίζονται στον παρακάτω Πίνακα 1. Αρχικά παραθέτουμε την αποδοχή σε προσβάσεις που «απαιτεί» κάθε εφαρμογή για να λειτουργήσει, είτε «ζητώντας» το από τον χρήστη, είτε όπως φαίνεται από την περιγραφή των εφαρμογών αυτών στο play store.

ΕΦΑΡΜΟΓΗ	**ΕΓΓΡΑΦΗ/ΟΤΡ**	**ΑΠΟΔΟΧΗ ΚΑΜΕΡΑΣ**	**ΑΠΟΔΟΧΗ ΜΙΚΡΟΦΩΝΟΥ**	**ΑΠΟΔΟΧΗ ΤΟΠΟΘΕΣΙΑΣ**	**ΑΠΟΔΟΧΗ ΕΓΓΡΑΦΗΣ ΣΥΣΚΕΥΗΣ**
STOP COVID-PROTEGO SAFE					
Covid-19-DXB Smart App	✓	✓	✓	✓	✓

NOVID			✓	✓	
SAFEPLACES				✓	✓
SWISS COVID					
IMMUNI					
CORONA-WARN-APP		✓			
TRACE TOGETHER	✓	✓		✓	✓

ΠΙΝΑΚΑΣ 1: ΣΥΝΟΛΙΚΕΣ ΑΔΕΙΕΣ ΠΡΟΣΒΑΣΗΣ ΕΦΑΡΜΟΓΩΝ

Στη συνέχεια, στον Πίνακα 2 παραθέτουμε συνολικά τα ευρήματα από το εργαλείο pi_maninthemiddle που αφορούν τις εφαρμογές που μελετήσαμε.

ΕΦΑΡΜΟΓΗ	**appID**	**UserId**	**Email**	**MAC**	**WiFi**	**Time Zone,Country**	**Μοντέλο και έκδοση Android**	**GAID**	**Android ID**
STOP COVID-PROTEGO SAFE	✓	✓	✓			✓	✓		✓
Covid-19-DXB Smart	✓		✓			✓	✓		

App									
NOVID	✓	✓		✓	✓			✓	
SAFEPLACES			✓			✓	✓		✓
SWISS COVID							✓		
IMMUNI							✓		
CORONA-WARN-APP	✓						✓		
TRACE TOGETHER	✓	✓	✓			✓	✓		

ΠΙΝΑΚΑΣ 2: ΣΥΝΟΛΙΚΕΣ ΠΡΟΣΒΑΣΕΙΣ ΕΦΑΡΜΟΓΩΝ

Παραθέτουμε συνολικά τα ευρήματά μας όσον αφορά τις πληροφορίες που αποκαλύπτουν οι παραπάνω εφαρμογές προς τη Google λόγω του GAEN (βλ .Πίνακα 3).

ΕΦΑΡΜΟΓΗ	**Firebase**	**Αιτήματα προς τη Google(Google.com/loc,Play.googlapis κ.α.)**
STOP COVID-PROTEGO SAFE	appId, fid,sdk version, χώρα,ζώνη ώρας	IP,Μοντέλο συσκευής,Email, android ID, email, userID,

Covid-19-DXB Smart App	Fid, appId,sdk version, χώρα,ζώνη ώρας	Ιστορικό χρήστη, σύνδεση με viber
NOVID	Fid, appId,sdk version, userID	UserID,
SAFEPLACES	Email, androidID,γλώσσα	Εισερχόμενα Email, androidID, email και μοντέλο συσκευής, ιστορικό χρήστη
SWISS COVID		
IMMUNI		
CORONA-WARN-APP		
TRACE TOGETHER	Fid, appID,ζώνη ώρας, userID	Email, serial number συσκευής, fingerprint, σύνδεση με Facebook graph

ΠΙΝΑΚΑΣ 3: ΣΥΝΟΛΙΚΕΣ ΔΙΑΡΡΟΕΣ ΤΩΝ ΕΦΑΡΜΟΓΩΝ ΛΟΓΩ ΤΟΥ GAEN

6.3 Έλεγχος Εφαρμογών ιχνηλάτησης χρησιμοποιώντας επιπλέον εργαλεία

6.3.1 Exodus Privacy

Το Exodus Privacy είναι ένας μη κερδοσκοπικός οργανισμός με επικεφαλής τους hacktivists. Σκοπός του είναι να βοηθήσει τους ανθρώπους να κατανοήσουν καλύτερα τα ζητήματα παρακολούθησης των εφαρμογών Android. Παρακάτω στον Πίνακα 4 θα δούμε 20 εφαρμογές ιχνηλάτησης και τον αριθμό των αδειών που απαιτούν καθώς επίσης και τον αριθμό των επικίνδυνων αδειών τους. Στη συνέχεια, θα αναλύσουμε τις άδειες αυτές και θα αναφέρουμε τα αποτελέσματα που βρήκαμε.

Εφαρμογή Ιχνηλάτησης	Συνολικός Αριθμός Trackers	Συνολικός Αριθμός Αδειών	Επικίνδυνες Άδειες Εφαρμογών
STOP COVID - ProteGO Safe	2	7	0
Covid19-DXB Smart App	3	23	9
NOVID	2	16	3
SafePlaces	1	37	5
SwissCovid	0	8	0
Immuni	0	6	0
Corona-Warn-App	0	8	1
Trace Together	2	15	3

CovidSafe(AU)	1	11	2
StopCovid	0	11	3
Aarogya Setu	2	13	3
CovidWatch	0	6	0
NHS COVID-19	0	8	1
Protect Scotland	0	6	0
CoronaSAFE	4	26	4
RadarCOVID	0	7	0
SmitteStop	0	22	2
Apturi Covid	2	8	0
CovidTracker	0	7	0

ΠΊΝΑΚΑΣ 4: ΣΥΝΟΛΙΚΕΣ ΠΡΟΣΒΑΣΕΙΣ ΕΦΑΡΜΟΓΩΝ

Μετά την ανάλυση που προηγήθηκε, 7 στις 20 εφαρμογές χρησιμοποιούν το «Google CrashLytics» (Το Crashlytics προσφέρει μια λύση αναφοράς σφαλμάτων για προγραμματιστές εφαρμογών), 9 εφαρμογές χρησιμοποιούν το «Google Firebase Anlalytics» (το Firebase προσφέρει λειτουργίες όπως αναλυτικά στοιχεία, βάσεις δεδομένων, ανταλλαγή μηνυμάτων και αναφορές σφαλμάτων),1 εφαρμογή χρησιμοποιεί τα «Huawei Mobile Services Core» »(Το HMS Core είναι μια συλλογή εργαλείων που έχουν δημιουργηθεί για συνεργάτες και προγραμματιστές εφαρμογών της Huawei. Περιλαμβάνει το κιτ διαφημίσεων, το κιτ Analytics, το κιτ τοποθεσίας και άλλα) και το com.onesignal(«OneSignal» τα οποία χρησιμοποιούν τα «com.huawei.hms.analytics | com.huawei.hms.location | com.huawei.hms.plugin.analytics | com.huawei.hms.plugin.ads).

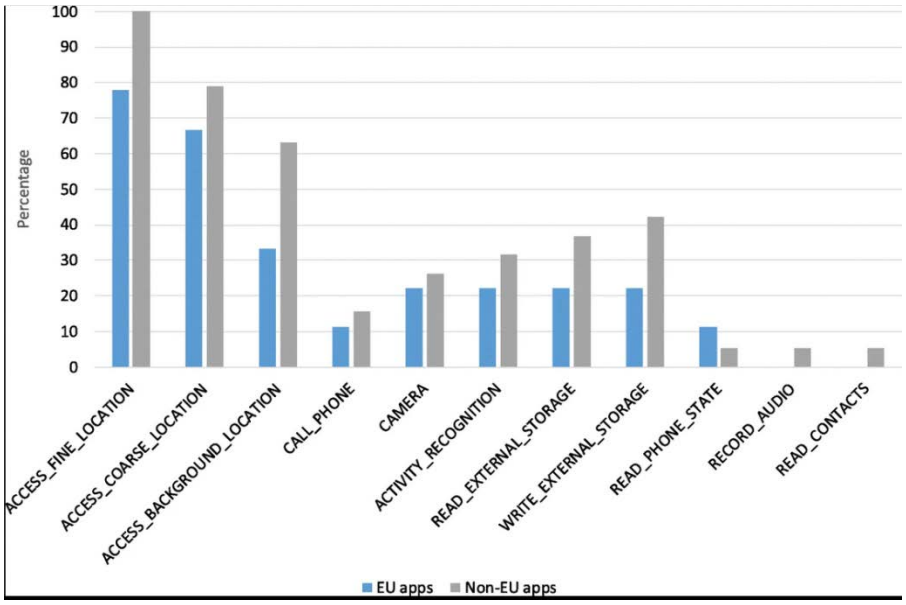
Από αυτές 10 εφαρμογές δεν είχαν κανένα tracker, ενώ 6 από αυτές δεν «ζητάνε» επικίνδυνες άδειες πρόσβασης ούτε tracker. Όμως 9 εφαρμογές «ζητάνε» επικίνδυνες άδειες όπως για παράδειγμα η εφαρμογή CoronaSAFE η οποία έχει πρόσβαση στην τοποθεσία του χρήστη μέσω GPS (android.permission.ACCESS_FINE_LOCATION), έχει πρόσβαση στις τηλεφωνικές κλήσεις (android.permission.CALL_PHONE) και έχει πρόσβαση στο τηλέφωνο (com.huawei.android.lancher.permission.WRITE_SETTINGS, com.oppo.lancher.permission.WRITE_SETTINGS).

Άλλη εφαρμογή με επικίνδυνες άδειες πρόσβασης είναι η Covid19-DXB Smart App, η οποία έχει πρόσβαση στην τοποθεσία τόσο μέσω διαδικτύου (android.permission.ACCESS.COARSE_LOCATION) όσο και μέσω GPS (android.permission.ACCESS_FINE_LOCATION), έχει πρόσβαση στην κάμερα, να βγάζει φωτογραφίες και βίντεο,(android.permission.CAMERA) να διαβάζει (android.permission.READ_CALENDAR) και να γράφει(android.permission.WRITE_CALENDAR) στο ημερολόγιο και τα δεδομένα μιας εξωτερικής κάρτας (android.permission.WRITE_EXTERNAL_STORAGE), να εγγράφει ήχο (android.permission.RECORD_AUDIO) και να εμφανίζεται στην κορυφή πάνω από άλλες εφαρμογές[6](android.permission.SYSTEM_ALERT_WINDOW).

Η εφαρμογή Trace Together της Σιγκαπούρης, όπως βλέπουμε στον Πίνακα 4, έχει δύο tracker και 3 επικίνδυνες άδειες πρόσβασης (ACCESS_FINE_LOCATION, CAMERA, READ_EXTERNAL_STORAGE). Πολλές μελέτες έχουν γίνει για αυτήν την εφαρμογή μιας και αποτελεί από τις πιο γνωστές εφαρμογές του κόσμου. Βασίζεται στο κεντρικοποιημένο σύστημα, μιας και μετά την εγκατάστασή της, ο χρήστης εγγράφεται με τον αριθμό τηλέφωνου του στον οποίο στέλνεται OTP για την πιστοποίηση της αυθεντικότητάς του και στη συνέχεια του ζητείται να τοποθετήσει τον αριθμό ταυτότητάς του ή του διαβατηρίου εάν επρόκειτο για τουρίστας.

Στην παρακάτω εικόνα (Εικόνα 65), βλέπουμε τις άδειες πρόσβασης εφαρμογών ιχνηλάτησης τόσο στην ΕΕ όσο και εκτός ΕΕ, σύμφωνα με έρευνες που έγιναν[15].

[6] Αυτό το παρατηρήσαμε και προηγουμένως



ΕΙΚΌΝΑ 65: ΣΥΝΟΛΙΚΕΣ ΠΡΟΣΒΑΣΕΙΣ ΕΦΑΡΜΟΓΩΝ

Παρατηρούμε ότι για την StopCovid-ProteGo Safe στην περιγραφή της εφαρμογής δεν αναγράφονται επικίνδυνες άδειες και ούτε εμφάνισε το exodus. Για την Covid19-DXB Smart App, αναγράφονται 7 άδειες στην περιγραφή και το exodus βρήκε 9 επικίνδυνες άδειες ενώ βρήκε 23 συνολικά. Για την NOVID, το exodus βρήκε 3 επικίνδυνες άδειες ενώ η περιγραφή της εφαρμογής εμφανίζει 2. Για το Safe Places, το exodus βρήκε 5 επικίνδυνες άδειες ενώ η περιγραφή εμφάνιζε 2 άδειες. Για τις Immuni και Swiss Covid δεν βρήκε επικίνδυνες άδειες και ούτε εμείς ανακαλύψαμε στην περιγραφή των εφαρμογών αυτών. Για την Corona-warn-app, το exodus βρήκε μια επικίνδυνη άδεια που περιγράφεται και στην περιγραφή της εφαρμογής. Τέλος για την Trace Together βρήκε 3 επικίνδυνες άδειες τις οποίες παρατηρούμε και στην περιγραφή της. Σε σύγκριση με το εργαλείο pi_maninthemiddle, βρήκαμε και εδώ ότι οι εφαρμογές χρησιμοποιούν το Google Firebase Analytics, βέβαια με το pi_maninthemiddle βρήκαμε περισσότερες συνδέσεις των εφαρμογών μιας όπως και προαναφέραμε τα αιτήματα είναι κρυπτογραφημένα και το εργαλείο μας μπορεί αποκρυπτογραφήσει τα περισσότερα από αυτά.

6.3.2 Lumen privacy monitoring app

Το Lumen είναι ένα ακαδημαϊκό ερευνητικό έργο με επικεφαλής το Διεθνές Ινστιτούτο Επιστήμης Υπολογιστών (ICSI), UC Berkeley και το IMDEA Networks. Χρηματοδοτείται από το Εθνικό Ίδρυμα Επιστήμης (NSF-National Science Foundation) και το Εργαστήριο Διαφάνειας Δεδομένων (Data Transparency Lab). Πρόκειται για μια εφαρμογή η οποία αναλύει την «κίνηση»

των εφαρμογών που είναι εγκατεστημένες στην κινητή συσκευή του χρήστη και αποκαλύπτει πώς επικοινωνούν οι εφαρμογές αυτές με υπηρεσίες παρακολούθησης, συλλέγοντας ευαίσθητες προσωπικές πληροφορίες για αυτόν. Ο χρήστης, έχει τη δυνατότητα να αποκλείσει ανεπιθύμητες ροές για μια εφαρμογή και να διαμορφώσει τις άδειες των εφαρμογών ώστε να διατηρήσει καλύτερα τον έλεγχο του ποιος έχει πρόσβαση στα προσωπικά του δεδομένα. Πρέπει να σημειωθεί ότι είναι πιθανό ορισμένες διαρροές στην τρέχουσα έκδοση του Android μας (σε αυτό το πείραμα χρησιμοποιήσαμε τη συσκευή μας με Android 9) ενδέχεται να μην είναι ανιχνεύσιμες, καθώς πολλές εφαρμογές χρησιμοποιούν κωδικοποίηση για να ανεβάσουν τα δεδομένα, ακόμη και για την τοποθεσία, και δεν υποστηρίζονται όλοι αυτοί οι μηχανισμοί στη δημόσια έκδοση του Lumen.

Μεταβαίνουμε λοιπόν στο google play store και «κατεβάζουμε» την εφαρμογή Lumen ώστε να ελέγξουμε τι είδους προσβάσεις έχουν οι εφαρμογές που αναλύσαμε προηγουμένως στην κινητή μας συσκευή και τι πληροφορίες αποκαλύπτουν και σε ποιους.

Η εφαρμογή δεν βρήκε «επικίνδυνες» διαρροές από τις εφαρμογών αυτές, αλλά βρήκε «επικίνδυνες» διαρροές προς τρίτες υπηρεσίες τις οποίες χρησιμοποιούν πολλές από τις παραπάνω εφαρμογές. Για παράδειγμα αναφέρουμε: το σειριακό αριθμό του android λογισμικού μας τον διαρρέει η υπηρεσία «facebook.com». Επομένως όταν οι εφαρμογές έχουν την επιλογή «κοινή χρήση με Facebook» (Share the app with Facebook), αποκαλύπτουν το σειριακό αριθμό του android λογισμικού μας. Τη ζώνη ώρας, που είναι μία μεσαίου επιπέδου επικινδυνότητας διαρροή, την αποκαλύπτει η υπηρεσία google.com, οπότε και οι εφαρμογές που κάνουν αιτήματα προς τη Google διαρρέουν μεσαίου επιπέδου επικινδυνότητας πληροφορίες της συσκευής. Η εφαρμογή viber αποκαλύπτει το μοντέλο της συσκευής, οπότε όσες εφαρμογές έχουν την επιλογή «κοινή χρήση με viber», συνδέονται με την υπηρεσία «rakuten.com» αποκαλύπτοντας το μοντέλο της συσκευής που είναι μια διαρροή χαμηλού επιπέδου επικινδυνότητας πληροφορία. Η συνδεσιμότητα της συσκευής και το μοντέλο της συσκευής είναι χαμηλού επιπέδου επικινδυνότητας πληροφορίες τις οποίες διαρρέουν οι υπηρεσίες της Google «googleapis.com» , «google.com» και «google.gr».

Συνοπτικά τα αποτελέσματα φαίνονται στον παρακάτω πίνακα 5.

ΥΠΗΡΕΣΙΑ	**Μεγάλη Επικινδυνότητα**	**Μεσαία Επικινδυνότητα**	**Χαμηλή Επικινδυνότητα**

Facebook.com	Android Serial	Installed Apps	Brand,connectivity, device model,sim provider
Rakuten.com		Installed Apps	Brand, device model
Google.com	Inbox.com,mail.com	Installed Apps,Time Zone	Connectivity, device model,build fingerprint
Googleapis.com			Connectivity, device model

ΠΙΝΑΚΑΣ 5: ΣΥΝΟΛΙΚΕΣ ΠΡΟΣΒΑΣΕΙΣ ΕΦΑΡΜΟΓΩΝ ΜΕ ΤΟ LUMEN

Η εφαρμογή Lumen βρήκε και μία επικίνδυνη διαρροή προς τον οργανισμό 172.217.23.110 όσον αφορά το δακτυλικό αποτύπωμα (device fingerprint) της συσκευής η οποία ανήκει στην Google.

Πρέπει πάντως να τονίσουμε και πάλι ότι η ελεύθερη εφαρμογή του Lumen Privacy Monitor δεν καταφέρνει να εντοπίζει κάθε εξερχόμενη από τη συσκευή μας πληροφορία εφόσον είναι κρυπτογραφημένη. Συνεπώς, για αυτό το λόγο τα ευρήματά μας, μέσω αυτού του εργαλείου, είναι περιορισμένα. Σε κάθε περίπτωση, επιβεβαιώνουν τα αντίστοιχα ευρήματα από τις άλλες εφαρμογές που χρησιμοποιήσαμε .

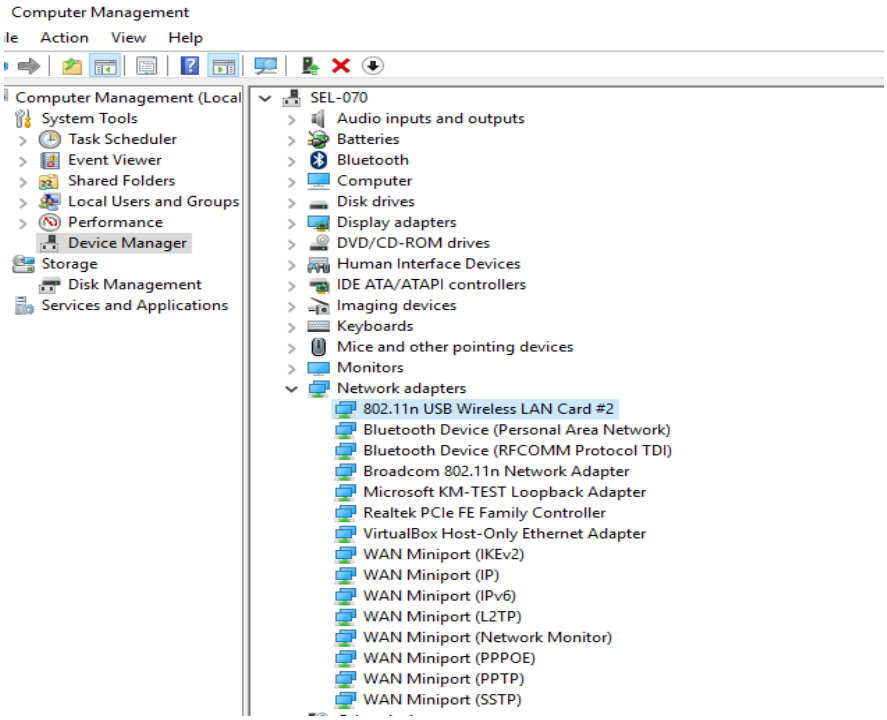
6.4 Προβλήματα που αντιμετωπίστηκαν κατά την έρευνα

Προβλήματα που αντιμετωπίστηκαν κατά τη διάρκεια εγκατάστασης και μπορούν να χρησιμοποιηθούν ως οδηγός για μελλοντική χρήση ήταν τα εξής :

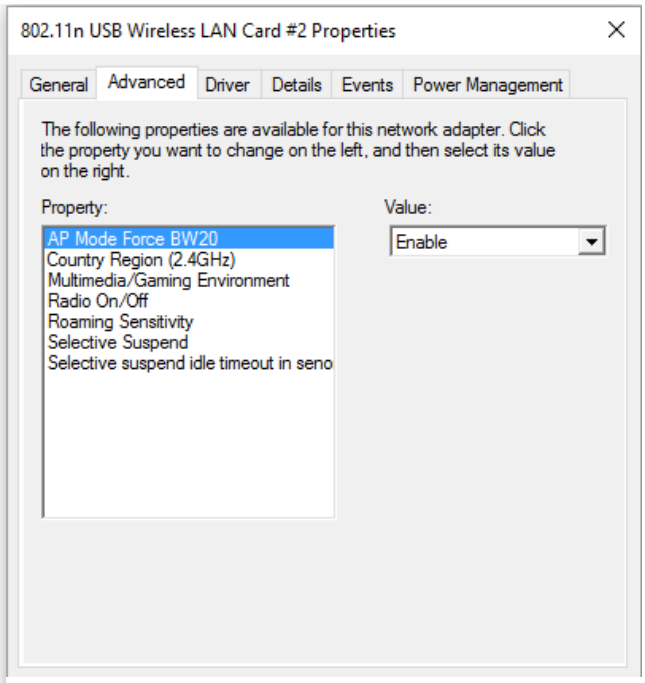
- Στην αρχή χρησιμοποιήσαμε ένα usb WiFi adapter της Mediatek το οποίο δεν συνδέθηκε ποτέ με το εικονικό περιβάλλον. Το εγχειρίδιο προτείνει να χρησιμοποιηθεί ένα usb WiFi adapter Ralink 5370 διότι ο driver=nl80211 που χρησιμοποιείται στο hostapd συνεργάζεται με αυτό ενώ

για να χρησιμοποιήσεις άλλο usb θα πρέπει να αλλάξεις τον driver=nl80211 στο hostapd κάτι το οποίο είναι πολύ δύσκολο να δουλέψει.

- Επειδή τη δεύτερη φορά που δοκιμάσαμε να συνδεθούμε, μας εμφάνιζε το μήνυμα «απαγόρευση πρόσβασης στο δίκτυο «pi_maninthemiddle», μεταβήκαμε στο computer management -> NetWork Adapters -> 80211.n usb WiFi adapter -> properties ->Advanced και αλλάξαμε όλες τις ρυθμίσεις σε «enabled» και ξανασυνδέθηκε όπως φαίνεται και στις Εικόνες 66 και 67:



ΕΙΚΌΝΑ 66: ΡΥΘΜΙΣΗ ΣΤΟ COMP.MANAGEMENT



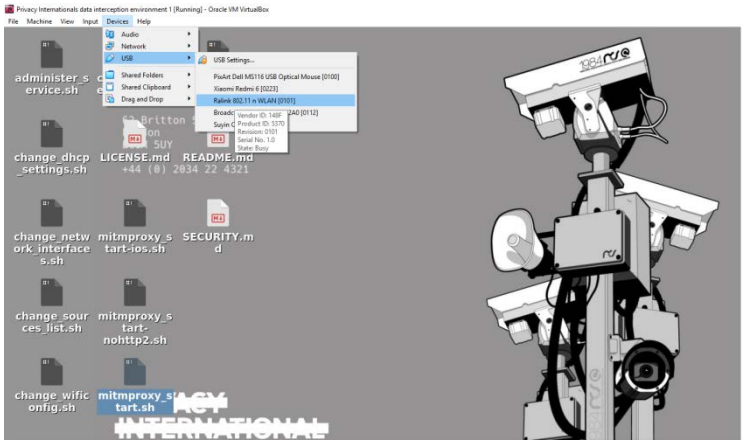
ΕΙΚΌΝΑ 67: ΡΥΘΜΙΣΗ ΣΤΟ USB RALINK

- Για να εμφανιστεί το ssid «pi_maninthemiddle» θα πρέπει να χρησιμοποιήσουμε την εντολή «sudo systemctl enable hostapd» και να κάνουμε επανεκκίνηση του εικονικού περιβάλλοντος. Μπορούμε ανά πάσα ώρα και στιγμή να ελέγξουμε την κατάσταση του hostapd με την εντολή "sudo systemctl status hostapd".

- Εάν η κινητή συσκευή κάνει looping μεταξύ των συνδέσεων και δεν μπορεί να συνδεθεί, τότε τρέχουμε τις εντολές «sudo systemctl networking restart» && «sudo systemctl dnssmasq restart».

- Ελέγχουμε πάντα αν η συσκευή είναι συνδεδεμένη στο virtual box, αν δεν είναι τη συνδέουμε. Όπως φαίνεται και στην Εικόνα 68:

- Ο οικοδεσπότης πρέπει να είναι συνδεδεμένος στο διαδίκτυο με NAT



ΕΙΚΟΝΑ 68: ΣΥΝΔΕΣΗ USB ΜΕ ΕΙΚΟΝΙΚΟ ΠΕΡΙΒΑΛΛΟΝ

Κεφάλαιο 7

ΕΠΙΛΟΓΟΣ

Η πανδημία του ιού Covid-19,οδήγησε στο μεγάλο lockdown με θύματα την ελευθερία των ανθρώπων αλλά και την ίδια την οικονομία παγκοσμίως.

Το εν λόγω θέμα έχει αποκτήσει εντονότατο ερευνητικό ενδιαφέρον ιδίως τους τελευταίους μήνες και αποτελεί πηγή προβληματισμού για αρμόδιους φορείς και αρχές. Τα αποτελέσματα της διατριβής αναμένεται να έχουν εξαιρετικό ενδιαφέρον όχι μόνο για την ερευνητική κοινότητα αλλά και για αρμόδιους φορείς της δημόσιας υγείας. Αν καταφέρουμε να ελαχιστοποιήσουμε τους κινδύνους που εγείρονται στη χρήση των εφαρμογών ιχνηλάτησης , ακόμα και να τους εξαλείψουμε, τότε συζητάμε για ένα φοβερά ενδιαφέρον τεχνολογικό επίτευγμα το οποίο όχι μόνο θα μειώσει την εξάπλωση του Covid-19 αλλά θα μπορεί να χρησιμοποιηθεί και μεταγενέστερα σε άλλους ιούς και να εξελιχθεί και για άλλες ασθένειες. Ήδη

πάντως, από την παρούσα διατριβή, διαφαίνεται η διαφορά της «κουλτούρας» ως προς την ιδιωτικότητα υπολοίπων χωρών σε σχέση με τις ευρωπαϊκές χώρες, αφού οι εφαρμογές που αναπτύχθηκαν στην ΕΕ επεξεργάζονται πολύ λιγότερη πληροφορία των χρηστών και των συσκευών τους. Σε κάθε περίπτωση βέβαια, εγγενείς αδυναμίες που υπάρχουν σε όλες τις «έξυπνες» εφαρμογές αναφορικά με την ιδιωτικότητα εμφανίζονται και εδώ – χαρακτηριστικό είναι το παράδειγμα της εφαρμογής της Πολωνίας όπου διαπιστώθηκαν αρκετές διαρροές δεδομένων. Η εν λόγω εφαρμογή, όπως και πολλές άλλες, στηρίζεται στο GAEN που όπως αναφέρει και το[3], το πρόβλημα είναι ότι εκατοντάδες προ-εγκατεστημένες εφαρμογές όπως το πρόγραμμα περιήγησης της Samsung και του MotoCare της Motorola σε συσκευές Android, έχουν πρόσβαση σε δυνητικά ευαίσθητες πληροφορίες που αποθηκεύουν οι εφαρμογές ιχνηλάτησης επαφών στα αρχεία καταγραφής συστήματος-ένα υποπροϊόν του τρόπου με τον οποίο οι προ-εγκατεστημένες εφαρμογές λαμβάνουν πληροφορίες σχετικά με τα αναλυτικά στοιχεία του χρήστη και αναφορές σφαλμάτων. Οπότε, πραγματικά δεν υπάρχει λόγος μια εφαρμογή ιχνηλάτησης κεντρικοποιημένη ή μη να στηρίζεται στο GAEN. Πρέπει επίσης, να δίνεται στον χρήστη η δυνατότητα να σταματά να χρησιμοποιεί τα Google play services λόγω των διαρροών που έχουν οι υπηρεσίες. Βέβαια αυτό είναι ένα πρόβλημα το οποίο είναι γνωστό και λίγο πολύ το έχουν αποδεχτεί όλοι όσοι γνωρίζουν το θέμα (αναφερόμαστε στις διαρροές πληροφοριών προς τη Google). Υπάρχει φόβος για τη διαρροή πληροφοριών από τις εφαρμογές ιχνηλάτησης και τελικά οι θεωρητικά "ακίνδυνες" εφαρμογές όπως το Gmail, το viber και το Facebook, είναι αυτές που πρέπει να θεωρούνται «επικίνδυνες». Άρα, οι εφαρμογές ιχνηλάτησης "υποφέρουν", όπως όλες οι "έξυπνες" εφαρμογές, από τα ίδια ελαττώματα και τις ίδιες ευπάθειες. Ως προς τους επιλεγέντες κρυπτογραφικούς αλγορίθμους, φαίνεται ότι όλες οι εφαρμογές υιοθετούν τα πρότυπα κρυπτογράφησης – με εξαίρεση το σύστημα Robert, που χρησιμοποιεί τον 3DES για τον οποίο ο NIST (National Institute Of Standards and Technology) έχει ανακοινώσει ότι σε λίγα χρόνια θα πρέπει να παύσει η λειτουργία του.

Πρέπει πάντως να επισημανθεί ότι, ακόμα και σε περιπτώσεις Ευρωπαϊκών χωρών, χρησιμοποιείται συχνά ο όρος «ανωνυμοποίηση» και «ανώνυμα δεδομένα» για να περιγράψει την επεξεργασία που συντελείται, το οποίο όμως, σύμφωνα με τον GDPR, δεν είναι απόλυτα ακριβές: εφόσον δημιουργούνται, έστω και για συγκεκριμένο χρονικό διάστημα, μοναδικά αναγνωριστικά ανά χρήστη με κάποια συμπληρωματική πληροφορία (που μπορεί να είναι από πληροφορία τοποθεσίας μέχρι πληροφορία συσκευής), ουσιαστικά πρόκειται για ψευδωνυμοποίηση (ενδεχομένως πολύ ισχυρής, που δεν επιτρέπει ευχερώς την ταυτοποίηση

του προσώπου, αλλά που όμως δεν μπορεί να αποκλειστεί πλήρως ως πιθανότητα για όλες τις περιπτώσεις).

Υπάρχουν πολλοί που αντιτίθονταν στην ιχνηλάτηση επαφών Covid-19 μέσω των εφαρμογών, λόγω του μεγάλου αριθμού λανθασμένων θετικών και αρνητικών αποτελεσμάτων. Ας αναρωτηθούμε όμως: *Αλήθεια πόσα διαγνωστικά τεστ βγαίνουν λανθασμένα κάθε μέρα;* Αυτό το γεγονός οδήγησε τις κυβερνήσεις στο να σταματήσουν να διενεργούν διαγνωστικά τεστ στον κόσμο; Η απάντηση είναι φυσικά πως όχι. Ας αναρωτηθούμε μάλιστα, τα εμβόλια που έχουν δημιουργηθεί έχουν 100% επιτυχία; Μάλλον όχι. Μάλιστα, έρευνες δείχνουν πως πολύς κόσμος αφενός μπορεί να πεθάνει από τα εμβόλια, αφετέρου δε δεν τον εξασφαλίζει από το να μην νοσήσει από τον ιό. Θεωρούμε λοιπόν ότι το μεγαλύτερο εμπόδιο στην ανάπτυξη ενός τέτοιου συστήματος, δεν είναι τα λανθασμένα αποτελέσματα που βγάζουν, αλλά ο κόσμος που δεν εμπιστεύεται τις κυβερνήσεις και τους προγραμματιστές των εφαρμογών κινητών συσκευών και δεν θα στηρίξει ένα τέτοιο σύστημα. Βέβαια από τη μία ο κόσμος δεν δέχεται καλοπροαίρετα τα νέα τεχνολογικά δεδομένα. Ας σκεφτούμε πόσα χρόνια έκανε ο κόσμος να δεχτεί το πλέον αναγκαίο «ebanking» γιατί φοβότανε μη χάσει τα χρήματά του και το πόσο ασφαλές είναι μια τέτοιου είδους οικονομική συναλλαγή. Από την άλλη, είναι λογικό να είναι φοβισμένος αφενός διότι έχει χάσει την εμπιστοσύνη του στις κυβερνήσεις και στους επιδημιολόγους, γιατί αναιρούν συνέχεια αυτά που υποστηρίζουν, αφετέρου έχει χάσει την εμπιστοσύνη του στους προγραμματιστές με όλες αυτές τις αποδοχές πρόσβασης στις εφαρμογές που ζητάνε και φοβάται μήπως τον παρακολουθούν. Η αλήθεια είναι ότι ο χρήστης που θα χρησιμοποιήσει τις εφαρμογές ιχνηλάτησης είναι ο συνειδητοποιημένος χρήστης, ο οποίος θα θελήσει να συμβάλλει στην καταπολέμηση του ιού, είναι εκείνος που θα κάνει τακτικά διαγνωστικά τεστ, που θα καλέσει την πολιτική προστασία για να δηλώσει ότι νόσησε και στην τελική είναι εκείνος που θα δεχτεί να εμβολιαστεί. Εκείνος ο χρήστης που αντιτίθεται σε όλα τα παραπάνω, είναι και αυτός που θα αντιταχθεί στη χρήση ενός τέτοιου εργαλείου ιχνηλάτησης επαφών.

Επομένως μάλλον το πρόβλημα δεν εναπόκειται στις εφαρμογές ιχνηλάτησης και μόνο, αλλά στη γενική αντίληψη του κόσμου και των πραγμάτων. Αν κάποια στιγμή όλα αυτά αλλάξουν, ίσως δεχτούμε τις εφαρμογές ιχνηλάτησης σαν αυτό που είναι, ένα μεγάλο τεχνολογικό γεγονός. Μια βοήθεια στην πολιτική προστασία στον «πόλεμο» κατά της πανδημίας. Μια ένδειξη ανθρωπιάς και φιλευσπλαχνίας προς τους συνανθρώπους μας και σε ένα καλύτερο αύριο για τα παιδιά μας. Για αυτό ακριβώς το λόγο, είναι σημαντικό μία εφαρμογή ιχνηλάτησης να διέπεται από πλήρη διαφάνεια και να σέβεται το θεμελιώδες δικαίωμα της προστασίας προσωπικών δεδομένων (δηλαδή να επεξεργάζεται πράγματι τα απολύτως απαραίτητα δεδομένα, χωρίς «διαρροές»

δεδομένων που εκφεύγουν του νομικού πλαισίου προστασίας δεδομένων), έτσι ώστε οι πολίτες να αποκτήσουν εμπιστοσύνη σε αυτή: με αυτόν τον τρόπο, θα αξιοποιείται από ολοένα και περισσότερους και συνεπώς, θα ενισχύεται η αποτελεσματικότητά της. Επομένως λοιπόν, τις εφαρμογές ιχνηλάτησης θα πρέπει να τις χρησιμοποιούμε για το κοινό καλό και το δημόσιο συμφέρον αρκεί βέβαια να υπάρχει διαφάνεια και με σεβασμό στα άτομα και στα προσωπικά τους δεδομένα.

Βιβλιογραφια

[01] L. Reichert, S. Brack, and B. Scheuermann, "A Survey of Automatic Contact Tracing Approaches," p. 20.

[02] N. Ahmed *et al.*, "A Survey of COVID-19 Contact Tracing Apps," *IEEE Access*, vol. 8, pp. 134577–134601, 2020, doi: 10.1109/ACCESS.2020.3010226.

[03] "Google Promised Its Contact Tracing App Was Completely Private—But It Wasn't – The Markup."https://themarkup.org/privacy/2021/04/27/google-promised-its-contact-tracing-app-was-completely-private-but-it-wasnt.

[04] S. Vaudenay, "Centralized or Decentralized? The Contact Tracing Dilemma," *Infoscience*, 2020. http://infoscience.epfl.ch/record/277809

[05] D. J. Leith and S. Farrell, "Contact tracing app privacy: What data is shared by Europe's GAEN contact tracing apps," *Testing Apps for COVID-19 Tracing (TACT)*, 2020.

[06] "A. Olbrechts, "Statement on the data protection impact of the interoperability of contact tracing apps," *European Data Protection Board - European Data Protection Board*, Jun. 17, 2020. https://edpb.europa.eu/our-work-tools/our-documents/statements/statement-data-protection-impact-interoperability-contact en.

[07] "ΚΑΝΟΝΙΣΜΟΣ (ΕΕ) 2016/ 679 ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒ ΟΥΛΙΟΥ - της 27ης Απριλίου 2016 - για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομέν ων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτώ ν και την κατάργηση της οδηγίας 95/ 46/ ΕΚ (Γενικός Κανονισμός για την Προστα σία Δεδομένων)," p. 88.

[08] A. Olbrechts, "Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak," *European Data Protection Board - European Data Protection Board*, Apr. 22, 2020. https://edpb.europa.eu/our-work-tools/our-documents/ohjeet/guidelines-042020-use-location-data-and-contact-tracing-tools en

[09] F. Aisec, "Pandemic Contact Tracing Apps: DP-3T, PEPP-PT NTK, and ROBERT from a Privacy Perspective," *IACR Cryptol. ePrint Arch.*, 2020.

[10] L. Reichert, S. Brack, and B. Scheuermann, "Privacy-Preserving Contact Tracing of COVID-19 Patients," p. 2.

[11] Tang, "Privacy-Preserving Contact Tracing: current solutions and open questions," arXiv:2004.06818 [cs], Available: http://arxiv.org/abs/2004.06818.

[12] "Secure multi-party computation," *Wikipedia*. Mar. 26, 2021, Available: https://en.wikipedia.org/w/index.php?title=Secure_multi-party_computation&oldid=1014294329.

[13]]Y. Gvili, "Security analysis of the COVID-19 contact tracing specifications by Apple Inc. and Google Inc.," *IACR Cryptol. ePrint Arch.*, vol. 2020, p. 428, 2020.

[14] S. Monogios, K. Limniotis, N. Kolokotronis, and S. Shiaeles, "A Case Study of Intra-library Privacy Issues on Android GPS Navigation Apps," in E-Democracy – Safeguarding Democracy and Human Rights in the Digital Age, vol. 1111, S. Katsikas and V. Zorkadis, Eds. Cham: Springer International Publishing, 2020, pp. 34–48

[15] M. Hatamian, S. Wairimu, N. Momen, and L. Fritsch, "A privacy and security analysis of early-deployed COVID-19 contact tracing Android apps," Empir Software Eng, vol. 26, no. 3, p. 36, doi: 10.1007/s10664-020-09934-4.

[16] J. Zang, K. Dummit, J. Graves, P. Lisker, and L. Sweeney, "Who Knows What About Me? A Survey of Behind the Scenes Personal Data Sharing to Third Parties by Mobile Apps," *Technology Science*.Available: /a/2015103001/.

[17] "Privacy International's data interception environment," Privacy International. http://privacyinternational.org/node/2732.

Παράρτημα Α

Συντομογραφίες

Α1. Συντομογραφίες

GDPR	General Data Protection Regulation
BLE	Bluetooth Low Energy
ACT	Application Contact Tracing
DP-3T	Decentralized Privacy Preserving Tracing
GAEN	Google Apple Exposure Notification
API	Application Programming Interface
EDPB	European Data Protection Board
ΕΕ	Ευρωπαϊκή Ένωση

IMEI	International Mobile Equipment Identity
ICO	Information Commissioner's Office
ΠΟΥ	Παγκόσμιος Οργανισμός Υγείας
ΓΚΠΔ	Γενικός Κανόνας Προστασίας Δεδομένων
HA	Health Authority
DPIA	Data Protection Impact Assessments
MAC	Media Access Control
SDK	Software Development Kit
NIST	National Institute Of Standards and Technology

Παράρτημα Β
Λίστα Πινάκων και Εικόνων

Β1. Λίστα Πινάκων

Β2. Λίστα Εικόνων